绿盟科技 安全事件响应观察报告

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

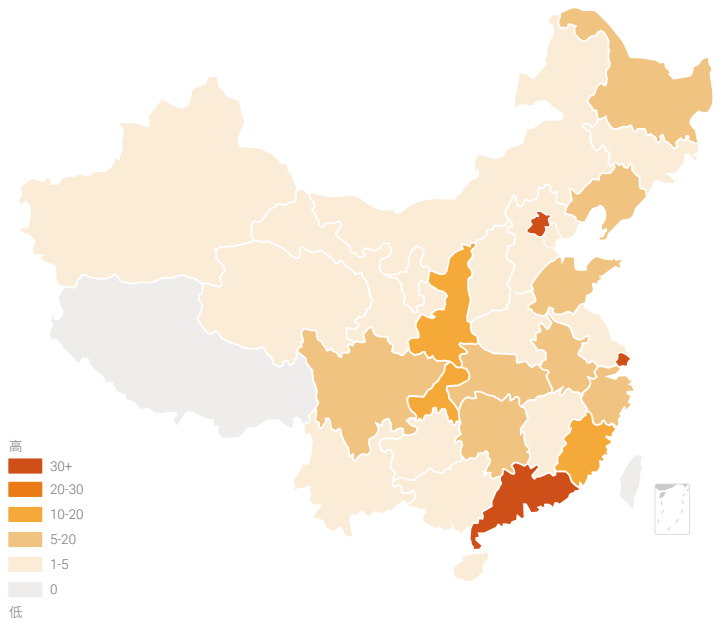
1

前言

2019 年 2 月中国互联网络信息中心发布的《中国互联网络发展状况统计报告》[1] 显示，截止 2018 年 12 月，中国网民规模达到 8.29 亿人，互联网普及率为 59.6%，互联网已经渗透到各行各业，直接影响着国家发展和人们的生产生活。随着互联网技术的发展，网络安全事件种类越来越多，攻击手段层出不穷，严重危及政府和企业的运转，极大影响了公众的社会生活。

绿盟科技应急响应团队 2018 年共处理来自全国各地的安全应急事件 338 起，涉及政府、运营商、金融、企业等行业，覆盖 30 个省份。安全事件地区分布如下图所示：

图表 1 安全事件地区分布

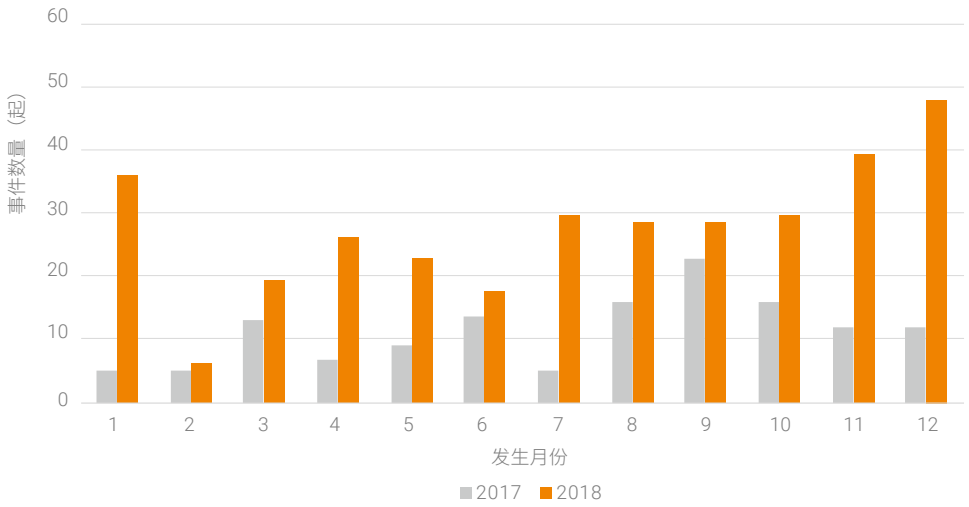


据统计，2018 年年初和年末发生的安全事件数量最多，远高于 2017 年同期处理事件数量。

1 中国互联网络发展状况统计报告 .http://www.cac.gov.cn/wxb_pdf/0228043.pdf

前言

图表 2 每月事件数量趋势



在对 2018 年处理的安全事件进行深入分析和整理的基础上，绿盟科技应急响应团队输出此报告。期盼更多的人能够关注安全事件现状，进一步提高安全意识；同时也希望各安全厂商齐心协力，共同为用户建设更加安全的网络环境。

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。

特别声明

本次报告中涉及的所有数据，均来源于绿盟科技的自有产品和合作伙伴产品，所有数据在进行分析前都已经过脱敏处理，不会在中间环节出现泄露，且任何与客户有关的具体信息，也均不会出现在报告中。

2

网络安全形势分析

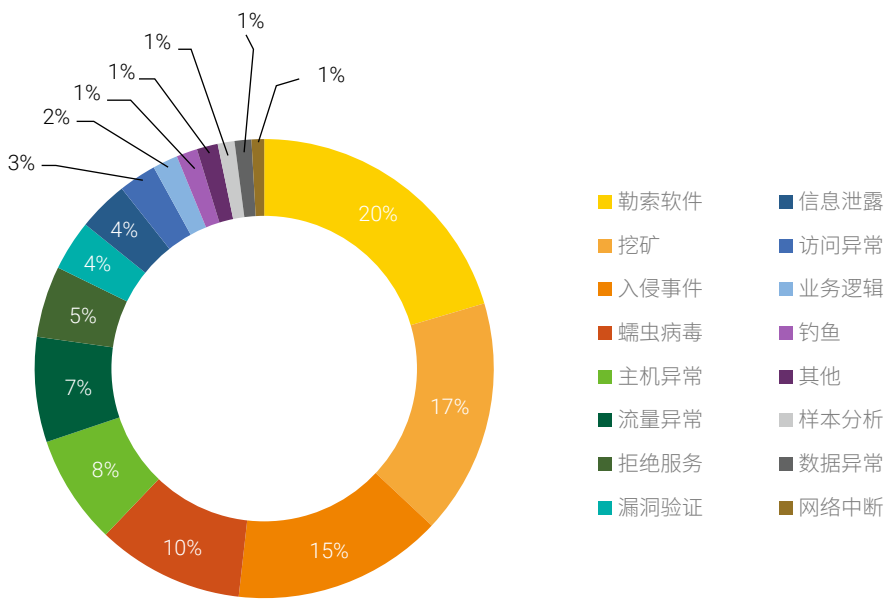
网络安全形势分析

随着网络安全形势的发展，越来越多的攻击者不再以炫耀技术能力为目的，而是以获取经济利益为行动向导。这些攻击运用的并非都是新技术，更多的是将现有的攻击工具、手法稍加改变，以突破企业防线。比起 2017 年，2018 年是相对平静的一年，如 MS17-010 等核弹级漏洞带来的阴影正渐渐淡去，但在这平静的表面下，黑色产业链也在默默壮大。

从整体上看：

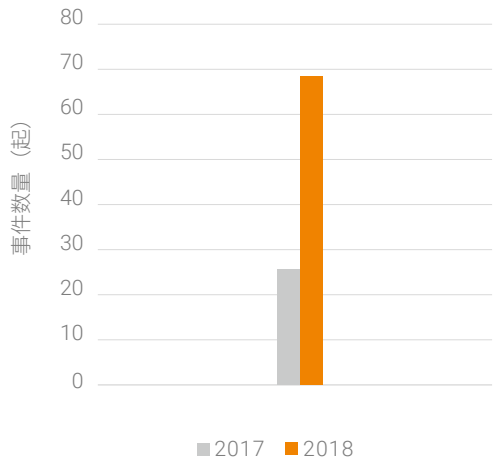
在绿盟科技 2018 年处理的安全事件中，勒索软件、挖矿和入侵类事件占比最高，分别为 20%、17% 和 15%。黑客的攻击目标和攻击手段一直在变，唯一不变的是攻击者对利益的追求。而虚拟货币因其不可追溯性成为攻击事件中资源套现的最好载体，黑客通过勒索和挖矿可以获得大量虚拟币，攫取高额的非法收入。典型的攻击场景主要有：虚拟币勒索、虚拟币盗窃、“挖矿”、诈骗等。安全事件占比如下图：

图表 3 事件类型分布



与去年相比，勒索软件的种类和数量成倍增涨，2017 年处理勒索病毒类安全事件 25 起，2018 年处理 69 起。

图表 4 勒索病毒安全事件数量对比



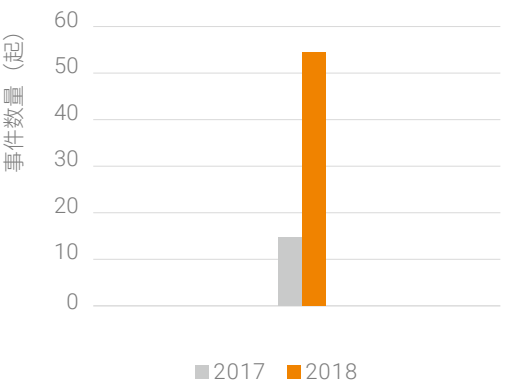
病毒种类由 2017 年的几种，发展到 2018 年的几十种；病毒在更新迭代速度上也是突飞猛进，并且呈现家族特征。其中 GandCrab、Cerber 等病毒已经超过五代，GlobeImposter 病毒也出现了第三代。

表 1 2017、2018 年活跃勒索病毒名称

年份	勒索病毒名称
2017 年	Wannacry、Petya、Crysis、数据库勒索、HDDCryptor、CRBR
2018 年	Wannacry、Petya、Crysis、数据库勒索、HDDCryptor、GlobeImposter、WannaMine、Rapid、lucky、GandCrab、.Wallet、Crysis、princess Locker、Cerber…

挖矿类安全事件由去年的 14 起增长到 56 起。在 2018 年中，挖矿病毒更多以蠕虫形式出现。

图表 5 挖矿类安全事件数量对比



从行业上来看：

政府单位服务器、网站一直很受黑客青睐，受到的攻击以 web 攻击为主。

运营商与网络应用服务和终端服务有着紧密的联系，这一特点使得运营商行业备受黑客瞩目。

金融行业由于其业务复杂、数据资产价值高等特点，安全事件的类型众多，容易成为境外黑客的攻击目标。

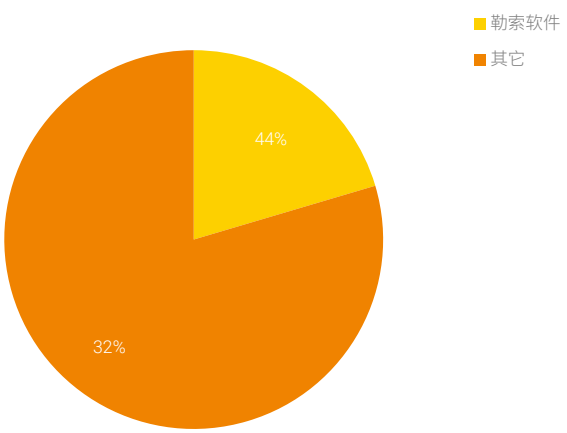
企业是受攻击的重灾区，其中尤以中小企业与中小互联网企业最为突出。中小型企业在网络安全方面投入不足，而产品销售维护又严重依赖互联网信息系统，网上公开的漏洞不能及时修补，导致大量的黑客攻击。

2.1 勒索软件仍是安全事件重点，并呈现家族化趋势

勒索病毒攻击早已不是什么新鲜手段，但勒索病毒和虚拟货币结合，就成了“黄金搭档”。2017 年 WannaCry 勒索病毒全球 “大屠杀”，让攻击者们意识到，这种“抢钱”方式安全且可靠。由此，利用勒索病毒谋取非法利益的安全事件愈演愈烈。

2018 年应急事件中，勒索软件类事件占比 20%，为众多事件类型之冠，可见勒索软件仍是网络攻击的重点。通过对今年勒索事件的处理及分析，发现勒索病毒在攻击目标、传播方式、技术门槛、新家族 / 变种、赎金支付方式等方面均呈现出新的特点。

图表 6 事件类型分布

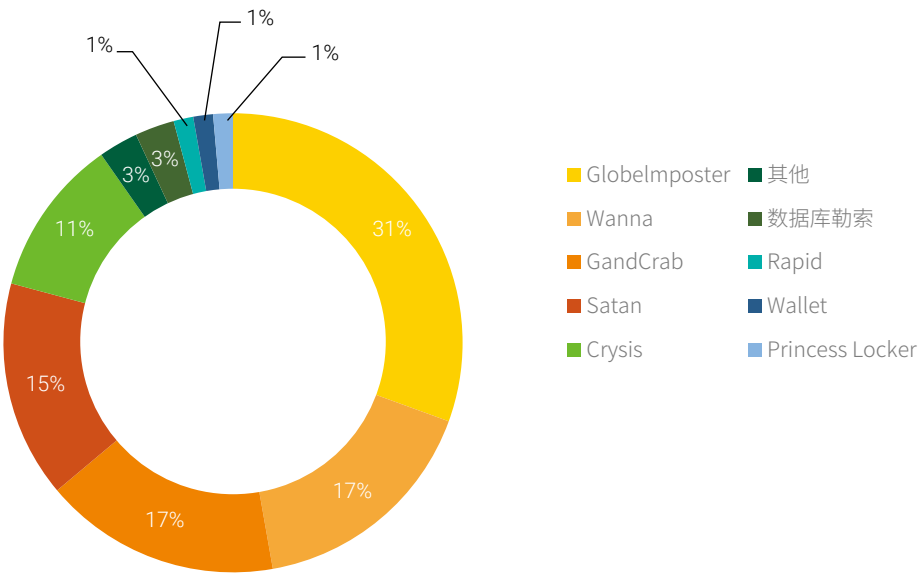


2.1.1 勒索病毒家族类型增多，变种更新更加频繁

从 2017 年 的 Wannacry，Petya，Satan 到 2018 年 的 Crysis，GandCrab，GlobeImposter，PrincesLocker，勒索病毒的家族类型在 2018 年变得更加丰富。同时单个病毒的更新次数也变得更加频繁，其中 Satan 在 2017 年 1 月首次出现，同年 12 月出现第二代变种，而在 2018 年分别在 5 月、6 月、11 月出现了三个变种更新，其样本的传播方式变得更加多样，勒索的赎金也相应有所增加； GandCrab V5 版本从 2018 年 9 月份面世以来，在短时间出现了 5.0、5.0.2、5.0.3、5.0.4、5.0.5 多个版本的变种。

下图为各应急事件中，各勒索病毒产生的应急事件汇总，可以发现在 2018 年里 GlobeImoposter、Wanna 系列、GandCrab、Satan 和 Crysis 几大家族包揽了 90% 的勒索事件，其中 GlobeImoposter 家族的事件占比高达 31%。

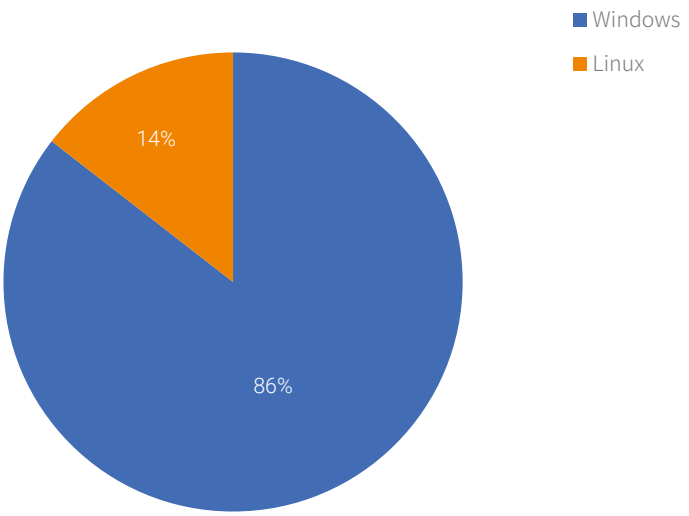
图表 7 勒索软件类型



2.1.2 Windows 服务器需重点关注，跨平台勒索病毒开始出现

不同于 2017 年 XOR、Billgates 等远控 DDoS 病毒家族大量出现，2018 年的主要角色变成了勒索病毒。勒索病毒的主要目标为各种 Windows 服务器，一方面，一般服务器中运行很多复杂的服务，很难第一时间对各种漏洞进行修补，另一方面，很多服务都存在弱口令的情况，种种原因都给攻击者提供了可乘之机。

图表 8 勒索软件传播平台

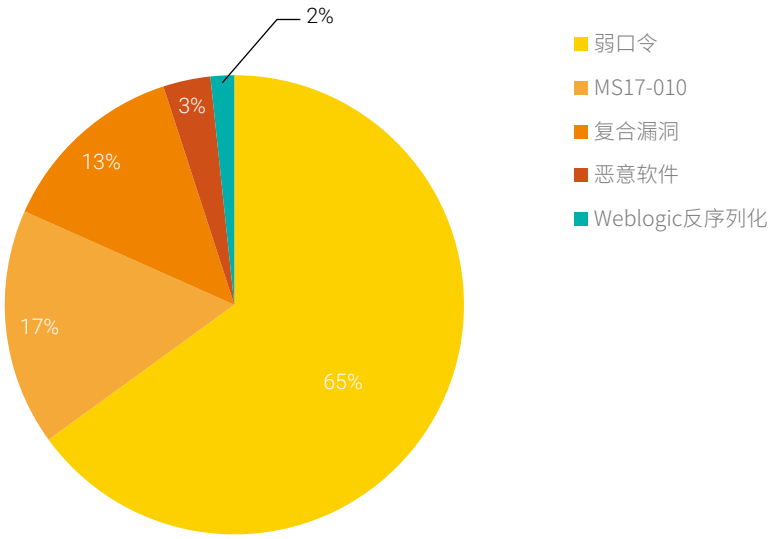


在 2018 年末出现了一种全新的可以在 Windows 和 Linux 双平台同时传播的勒索病毒，经过分析发现该病毒属于 Satan 变种（加密后缀名为 Lucky），之后勒索病毒跨平台传播也许会将成为一种新趋势。

2.1.3 RDP 弱口令暴力破解成为主流攻击方式

勒索软件的传统传播方式一般为钓鱼邮件、网页挂马、程序捆绑。在 2018 年，新出现的 GlobeImposter、GandCrab 等病毒使用的 RDP 口令爆破的传播方式成为了主流。下图为 2018 年绿盟科技应急响应团队处理的勒索应急事件的利用漏洞类型，其中弱口令占比 65%，可见 RDP 口令爆破攻击占据了主导地位。

图表 9 勒索软件利用漏洞类型



2.1.4 病毒制作门槛降低，传播方式蠕虫化

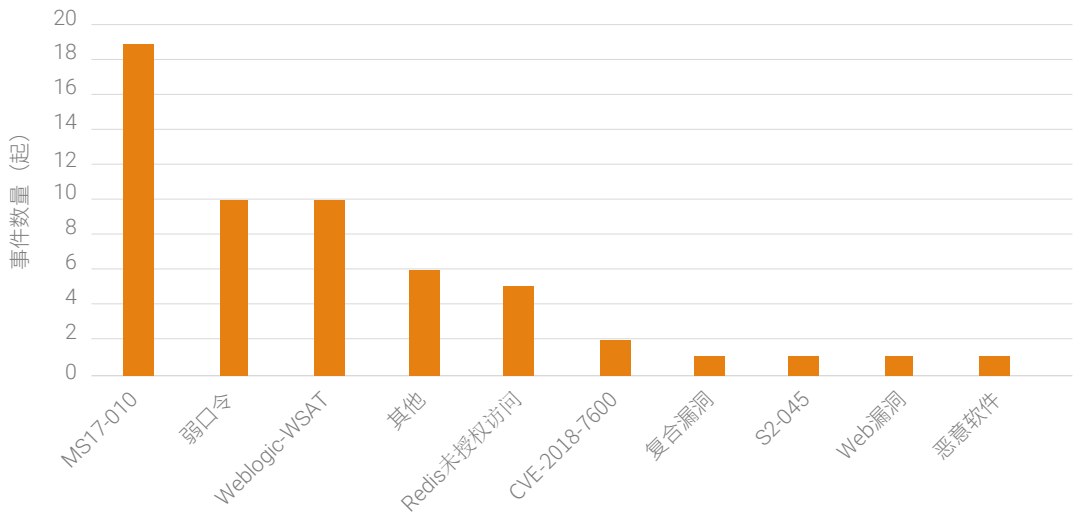
2018 年勒索病毒频繁出现使其成为了病毒舞台的主角。所谓“重金之下必有勇夫”。由于勒索病毒带来的利润极其可观，使很多病毒开发者竞相制作勒索病毒，所以出现了病毒质量良莠不一的情况。例如 2018 年 12 月出现的“微信勒索”仅使用固定密钥对文件进行异或加密，通过简单的脚本即可实现文件解密。由于微信支付容易溯源攻击者，12 月 5 日病毒开发者就已落网。

勒索程序蠕虫化已成为勒索病毒发展的一大趋势，勒索软件多数利用 RDP 暴力破解以及通过多种漏洞利用进行蠕虫传播。相比 2017 年 WannaMine 使用单一的 MS17-010 漏洞进行传播，今年流行的 Satan 更像是漏洞利用的百科全书，同时使用“JBoss 反序列化漏洞”、 “WebLogic WLS 组件漏洞（CVE-2017-10271）”、“Windows SMB 远程代码执行漏洞 MS17-010”、“Apache Struts2 远程代码执行漏洞 S2-045”等近 10 种已知漏洞进行传播。并且相对于 Satan 的上一版本，新版 Satan 变种已支持 Windows、Linux 的跨平台传播，虽然当前 Satan 新版变种稳定性较差，但是在 2019 年很有可能出现健壮的 Satan 变种。

2.2 挖矿病毒利用多种漏洞传播

2018 年，绿盟科技应急响应团队共处理挖矿事件 56 起，其中使用门罗币进行挖矿的事件占据绝大部分，高达 81%；已处理的挖矿事件中攻击手段也多种多样，其中，利用永恒之蓝漏洞的事件 19 起，利用 WebLogic 组件漏洞的事件 10 起、利用弱口令入侵挖矿事件 10 起、Redis 入侵挖矿事件 5 起；在所有挖矿事件中，涉及的病毒及挖矿工具：WannaMine 家族 18 起、cpuminer5 起、Redis Miner4 起、DDG4 起、powerghost 8 起。目前主流的恶意挖矿病毒为 WannaMine、powerghost 等。

图表 10 挖矿事件利用漏洞



2.2.1 WannaMine 挖矿病毒依然流行

2018 年由 WannaMine 挖矿病毒导致的应急事件相比 2017 年大幅减少，但是，该类型事件依然发生于部分企业，其中卫生、教育行业较为突出。该病毒依旧利用 MS17-010 微软文件共享协议漏洞，进行传播并挖矿。尽管官方补丁早已推出，由于企业人员安全意识不足、安全体制不完善等原因，此类事件仍时有发生。

2.2.2 门罗币成为挖矿病毒的首选币种

门罗币作为隐匿性最强的加密货币，一直备受匿名用户的青睐，一般的匿名，比特币就可以做到，

但是要想做到完全的匿名，目前来看非门罗莫属。门罗币完全匿名的特性，使得其与洗钱行业“纠缠不清”，无章可循也使其在暗网购买非法商品变得更加隐蔽。然而正是这些特性，使它在经历了多年的市场洗礼后仍屹立不倒，并且在加密货币中占据主流地位。市面上门罗币流通量的 5% 都是挖矿病毒生产的。

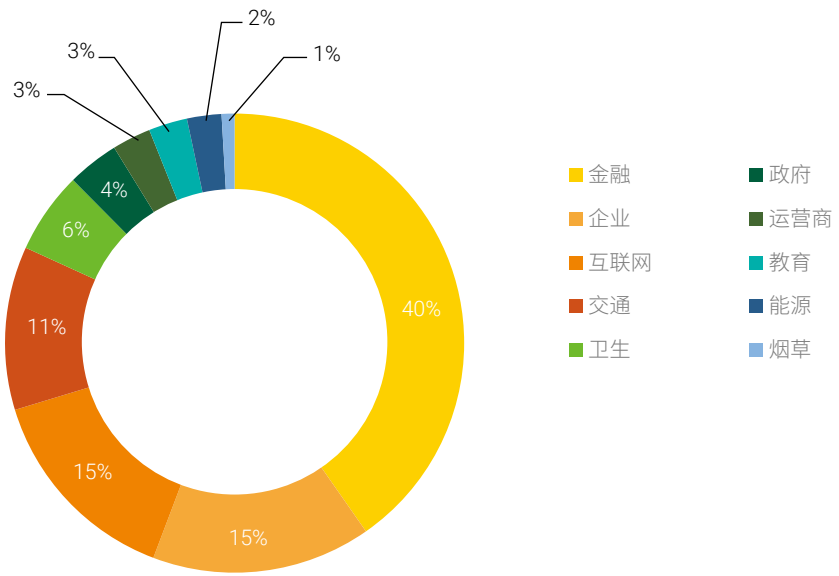
由于利益驱使，挖矿应急事件也呈逐年上升趋势，2018 以来，绿盟科技支持的挖矿应急事件的比例已经达到了 17% 之多，而在所有的挖矿事件中，有 81% 是门罗币挖矿。

2.3 网络威胁行业特征显著

今年处理的安全事件中，金融、企业、政府、运营商和互联网占比最高，上述几种行业体量较大、分布较广、数据更为敏感，往往会成为攻击的重点对象。由于各个行业的业务特性不同，安全事件在不同行业中呈现的侧重点有所区别，但勒索软件、挖矿、入侵事件在不同行业均有所表现。

其中勒索软件类事件重点影响金融、企业、政府、运营商、能源等行业；挖矿类事件影响金融、交通、政府等行业；入侵类事件影响政府、金融、互联网行业；主机异常类事件在企业、互联网行业影响较大。

图表 11 行业类型分布

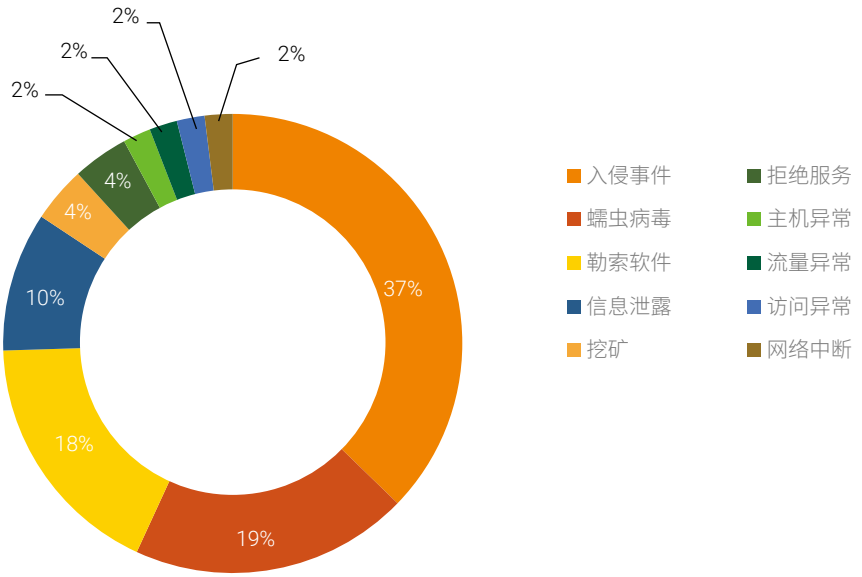


2.3.1 政府部门 Web 服务器成为攻击重点

互联网技术的发展正在引发一场电子政务安全防护领域的革新，网络在带来便利的同时，也存在潜在的安全隐患。政府部门由于掌握的信息敏感性高，让其成为黑客的重要攻击目标之一。

绿盟科技 2018 年处理的安全事件中，政府部门的入侵事件占比 37%，其中多为网页篡改类事件，Web 服务器已成为攻击的重点。

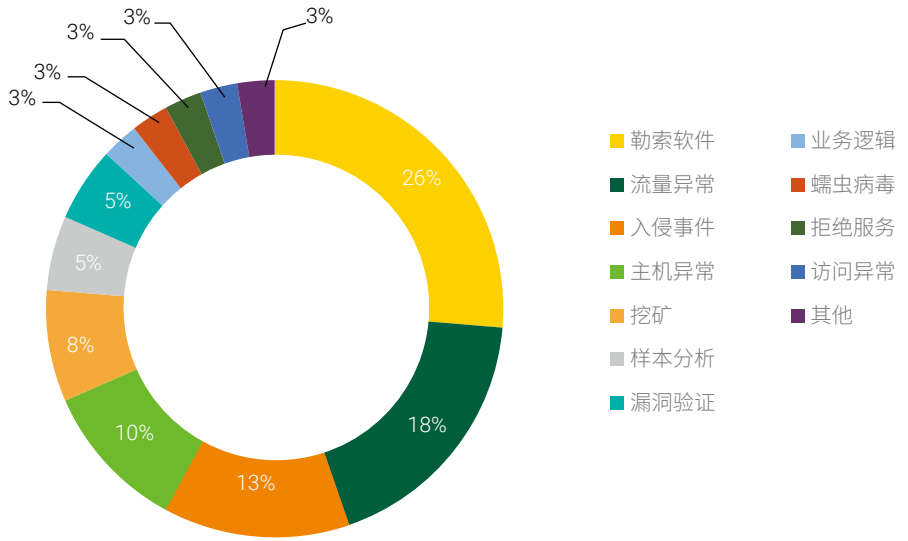
图表 12 事件类型分布 - 政府部门



2.3.2 运营商需着重关注勒索软件、流量异常类安全事件

运营商作为网络设施的建设、运营和维护单位，在网络层面承担了基础和关键性的角色。同时，运营商又与网络应用服务和终端服务有着紧密的联系，这一特点使得运营商行业备受黑客瞩目。总体上今年运营商的安全事件比去年有所减少，但勒索软件类安全事件却有所增长，流量异常事件仍是运营商的关注重点。

图表 13 事件类型分布 - 运营商



2.3.3 金融机构已成为网络犯罪的主要目标

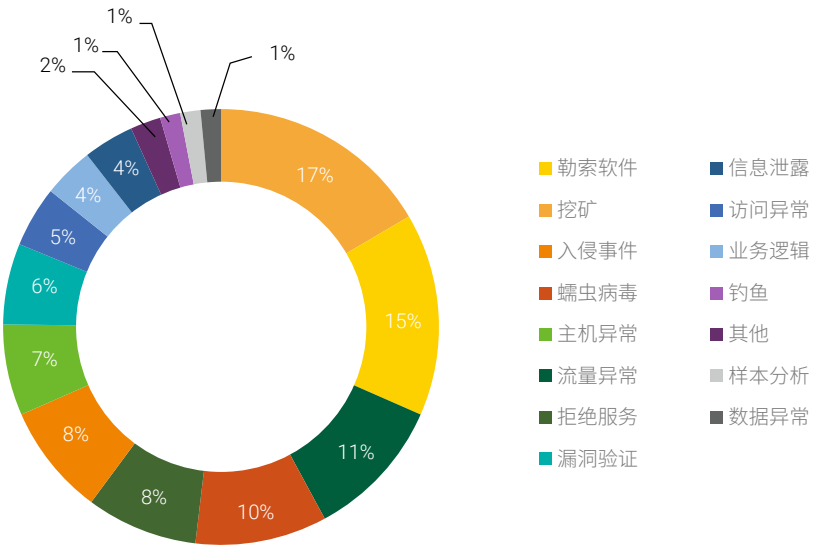
金融行业是我国网络安全重点行业之一，由于其业务复杂、数据资产价值高等特点，金融机构已经成为网络犯罪的主要目标。金融行业在今年处理的安全事件中占比高达 40%，且事件的类型众多，其中挖矿事件和勒索事件分别占比 17% 和 15%。

2018 年 11 月底，国内多个金融客户感染了跨平台的勒索病毒，该病毒是 Satan 勒索病毒的变种版本，利用了永恒之蓝和多种中间件漏洞可以在 Linux 和 Windows 平台进行蠕虫式传播，感染主机后会下载门罗币挖矿程序和勒索软件。

自 12 月 11 日起，有疑似“Anonymous”黑客组织账号在推特上发动代号为 OpIcarus 的攻击行动，并称已攻陷部分国外银行。在其发布的攻击目标清单中，包含部分国内银行网站。从网络信息判断，攻击形式以 DDoS 分布式拒绝服务攻击为主。

金融行业对于声誉尤其看重，因此除了占据主流的勒索软件、挖矿和入侵事件外，还关注信息泄露、业务逻辑等影响自身声誉的安全事件。

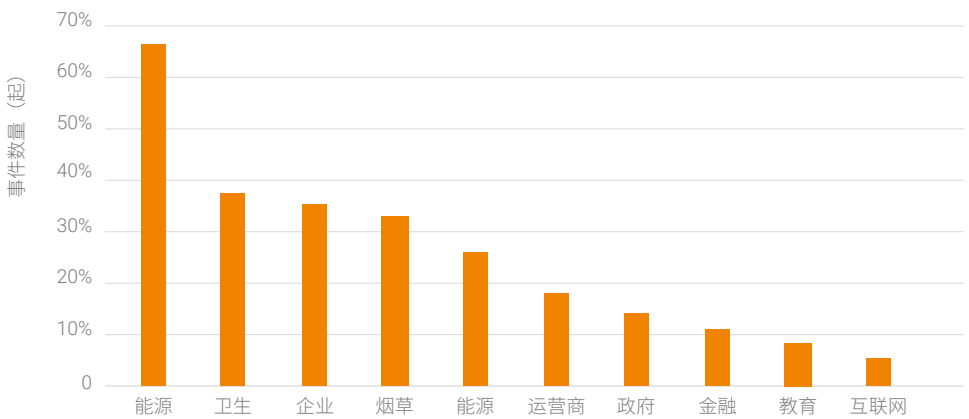
图表 14 事件类型分布 - 金融行业



2.3.4 企业的勒索事件占据绝对比重

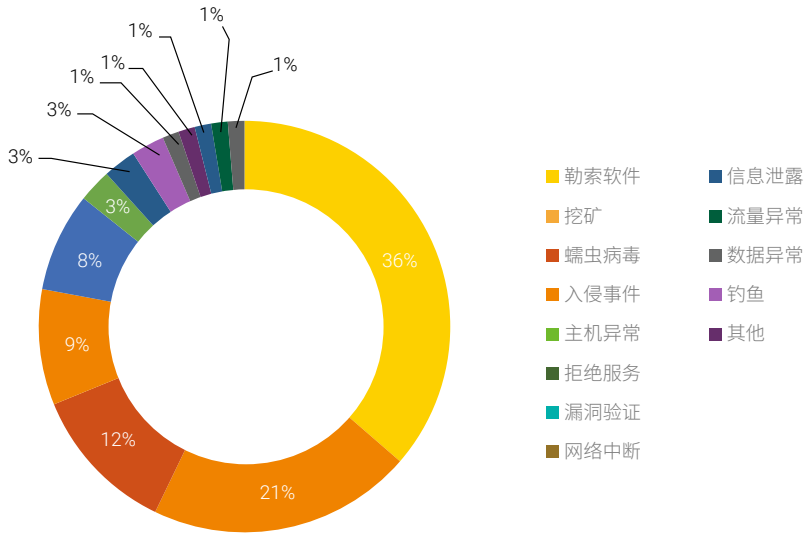
能源、教育、卫生等行业较为关注业务的连续性，对于影响业务运行和自身声誉的安全事件更为重视。这些行业的数据文件关系着业务的正常运行，且具有较高的价值，被加密后很可能影响业务，因此一旦感染勒索病毒主动支付赎金的意愿较高。黑客受到利益驱动，会对这些行业进行针对性的攻击。

图表 15 勒索软件影响行业



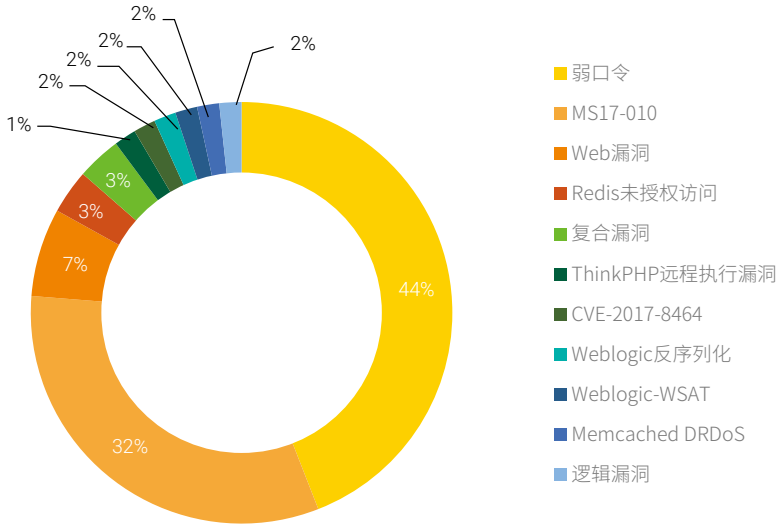
今年处理的安全事件中，勒索软件类占据了企业行业事件的绝对比重（36%）。

图表 16 事件类型分布 - 企业



企业行业中利用弱口令类漏洞的事件占比 41%，远高于其他行业。可见企业需要提高安全投入，完善网络安全管理工作，提高员工的安全意识。

图表 17 企业事件漏洞分布图



2.4 脆弱系统将面临越来越多的攻击

随着计算机系统的不断完善，各种应用软件也是层出不穷，伴随着应用软件的增多，互联网资产暴露的情况也越来越严重。攻击者可以使用 Nmap、Masscan、Metasploit 等工具来获取互联网上暴露出来的公共资产，相应的服务也就成为了攻击者攻击的目标。诸如 RDP、SSH、Redis、Memcached、Tomcat、FTP 等软件的使用，导致各种攻击也是屡见不鲜。

2.4.1 1Day 漏洞抢占肉鸡资源

由于 0Day 漏洞挖掘难度高、购买代价大等原因，攻击者很少将其用于批量化的攻击。而对于已经通过各种途径曝光的 1Day 漏洞，攻击者往往能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。从漏洞披露到安全事件全面爆发都有一定的周期，在安全事件爆发之前大多数企业并不密切关注和跟进漏洞，也没有及时更新相关补丁，导致在漏洞公布后的短时间内便被入侵。例如，2018 年 1 月，互联网上出现利用 WebLogic-WLS 组件远程命令执行漏洞进行挖矿的事件，短时间内大量爆发，影响到金融、运营商等多个行业。

如果用户及时关注厂商发布的漏洞和事件预警（如绿盟科技安全预警公众号：nsfocus_secwarning），在第一时间做好防范工作，可以有效防止此类攻击。

下面列举了几个 18 年应急过程中常见的新发漏洞：

表 2 WebLogic 反序列化漏洞

WebLogic 反序列化漏洞（CVE-2018-2628）	
影响范围	Oracle WebLogicServer 10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3
类型	远程代码执行、反序列化
危害	攻击者可以在未授权的情况下通过 T3 协议对存在漏洞的 WebLogic 组件进行远程攻击，并可获取目标系统所有权限。

表 3 Struts2-057 远程命令执行漏洞

Struts2-057 远程命令执行（CVE-2018-11776）	
影响范围	Struts 2.3 – Struts 2.3.34 Struts 2.5 – Struts 2.5.16
类型	远程命令执行
危害	Struts2 在 XML 配置中如果 namespace 值未设置且（Action Configuration）中未设置或用通配符 namespace 时可能会导致远程代码执行。

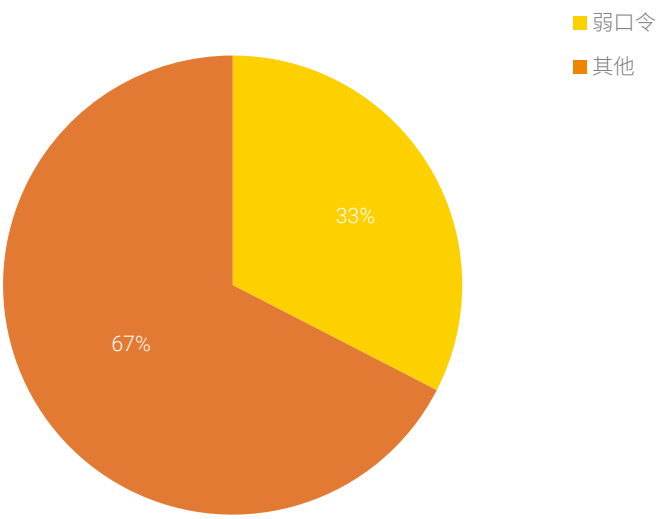
表 4 Drupal 远程命令执行漏洞

WebLogic 反序列化漏洞（CVE-2018-2628）	
影响范围	Drupal 6.x、Drupal 7.x、Drupal 8.x 均受此漏洞影响
类型	远程代码执行
危害	攻击者在 " 可渲染数组 " 中插入构造恶意代码，恶意代码通过 POST 方法将含有恶意代码的 " 可渲染数组 " 提交到 drupal 系统中。页面渲染流程中，" 可渲染数组 " 中携带的恶意代码，最终调用方法将 " 可渲染数组 " 中的恶意代码取出，传入 call_user_func 函数，导致恶意代码被执行。

2.4.2 NDay 漏洞持续威胁用户安全

在 2018 年处理的事件中，由历史漏洞造成的事件占比 34%，常见漏洞有 MS17-010、Struts2-045、Struts2-046、反序列化等。NDay 漏洞利用攻击事件往往是由于用户缺乏安全意识，没有更新或者安装官方的补丁，导致黑产从业者可以轻松地通过网上公开的漏洞利用代码进行攻击，攻击成本较低，造成危害较大。

图表 18 脆弱性分布统计图



下面列举了几个应急过程中常见的 NDay 漏洞：

表 5 MS17-010 永恒之蓝

MS17-010 永恒之蓝	
影响范围	Windows Vista，Windows Server 2008，Windows 7，Windows Server 2008 R2，Windows 8.1，Windows Server 2012 和 Windows Server 2012 R2，Windows 10，Windows Server 2016
类型	远程代码执行
危害	攻击者向 Windows SMBv1 服务器发送特殊设计的消息，最严重的漏洞可能允许远程执行代码。

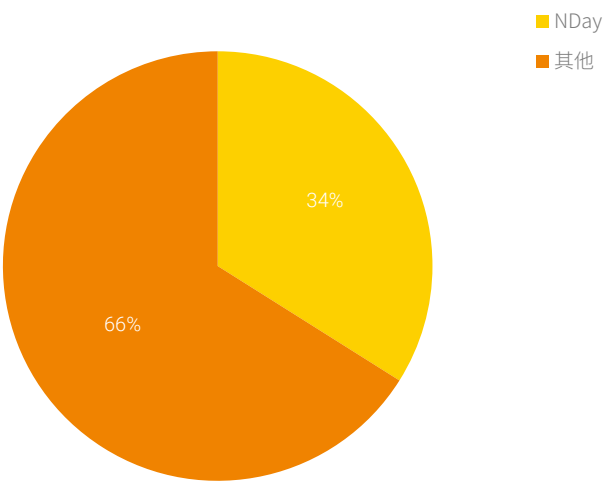
表 6 Struts2-045 远程命令执行

Struts2-045 远程命令执行	
影响范围	Struts 2.3.5 – Struts 2.3.31 Struts 2.5 – Struts 2.5.10
类型	远程命令执行
危害	Struts 使用的 Jakarta 解析文件上传请求包不当，当远程攻击者构造恶意的 Content-Type，可能导致远程命令执行。

2.4.3 弱口令仍是安全事件“高发地”

利用弱口令进行攻击的安全事件占 2018 年处理事件总数的 33%，可见弱口令是安全事件高发的重要原因之一。针对 RDP、SSH、Redis、Memcached、Tomcat 等服务的攻击类型中，弱口令尤为突出，攻击行业覆盖运营商、企业、政府、金融、能源等多种行业类型，攻击类型包括蠕虫、暴力破解、人工渗透等多种手段。在弱口令的攻击中，RDP 暴力破解成为主要的入侵手段。

图表 19 脆弱性分布统计图



3

安全处置建议

安全处置建议

在安全领域，最为基础的安全管理防护措施发挥着最为重要的作用，绝大多数的安全事件可以通过基础的控制措施进行防护：

- 有效和更新的管理制度和流程机制
- 有效的网络边界隔离与防护
- 定期 / 不定期的安全评估
- 严格的权限账户管控
- 配置操作规范和安全审计
- 安全漏洞的发现与修补
- 桌面终端安全防护
- 持续的内部人员安全培训
- 第三方服务及供应链的安全管控
- 安全应急预案编制与应急演练

4

典型安全事件应急处置案例分析

4.1 勒索软件典型案例

4.1.1 GlobeImposter 家族

在绿盟科技 2018 年中的全部应急事件中，勒索病毒事件应急占据了最高的比重，而在各个勒索病毒样本里面 GlobeImposter 勒索病毒正是其中最为活跃的一个样本。

4.1.1.1 背景介绍

GlobeImposter 又称：江湖骗子，早期主要通过钓鱼邮件方式进行传播感染，感染方式为通过邮件附件中的 js 文件执行并下载最终的勒索病毒。GlobeImposter 勒索病毒早在 2017 年 11 月就首次爆发。到 2018 年 3 月发现了 GlobeImposter 勒索病毒的变种，新变种增加了免杀技术和痕迹清理，被命名为 GlobeImposter2.0 版本。随后在 8 月出现了 3.0 的版本，其功能与 2.0 版本时相差不大，主要增加了文件加密后的后缀名类型，并且出现了通过人工渗透进行病毒传播的情况。

4.1.1.2 事件分析

4.1.1.2.1 传播方式

GlobeImposter 病毒本身不具备传播性，主要通过垃圾邮件和 RDP 暴破植入传播。

第一步：密码获取。

利用 mimikatz.exe 获取本机的所有用户名、密码；

获取其他密码：浏览器、wifi、数据库、邮箱。（passrecenc 工具套装）。

https://github.com/AlessandroZ/LaZagne

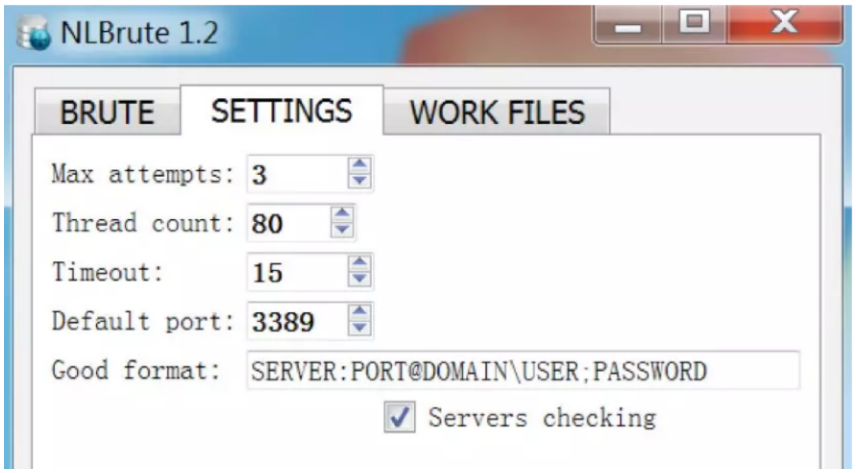
第二步 扫描 3389：

利用局域网扫描工具 nasp.exe，扫描 3389 端口

NetworkShare v.2 扫描内网 B 段共享。

第三步：NLBrute.exe 爆破 RDP。

图 1 NLBrute 1.2



4.1.1.2.2 病毒行为

1. 拷贝病毒自身到：%AppDataLocal%\{Malware Name}.exe
2. 在 %SystemRoot%\Users\Public\ 目录生成 RSA 公钥的 SHA256 的值文件，形式如：B26A340109A0081ADF57D63647533B8681DC0B8E159BE 052385ED4024E9CFFBC
3. 添加注册表实现自启动：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce BrowserUpdateCheck = %Application Data%\{Malware name}.exe
4. 加密文件路径下，生成勒索提示信息文件： how_to_back_files.html
5. 初始化完成开始执行加密操作，GlobeImposter1.0 在加密前会遍历进程并结束相关的进程，2.0 版本后取消此功能，病毒会直接进行加密文件的操作
6. 加密完成后，在临时目录下生成一个随机文件名的 .bat 文件，如：tmpADF9.tmp.bat，清除 RDP 登录的历史记录，然后自删除。

4.1.1.3 排查方式

1. 定位时间：

   查看第一个被加密文件前后的时间。

2. 定位进程：

   查看入侵时间前后创建或修改的可执行文件。

   查看占有 CPU 较多的进程。

3. 定位启动项：

   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

4. 定位攻击源：

   RDP 暴力破解成功时，包括四条审核成功日志，对应事件 ID 为：4672、4624、4776、4634，可从日志信息中获取攻击源 IP、登陆账号名等信息。

4.1.1.4 专家建议

- 尽量避免 RDP 端口对外开放，利用 IPS、防火墙等设备对 RDP 端口进行防护；
- 开启 Windows 系统防火墙，通过 ACL 等方式，对 RDP 及 SMB 服务访问进行加固；
- 通过 Windows 组策略配置账户锁定策略，对短时间内连续登陆失败的账户进行锁定；
- 加强主机账户口令复杂度及修改周期管理，并尽量避免出现通用或规律口令的情况；
- 修改系统管理员默认用户名，避免使用 admin、administrator、test 等常见用户名；
- 安装具备自保护的防病毒软件，防止被黑客退出或结束进程，并及时更新病毒库；
- 加强企业员工安全意识培训，不轻易打开陌生邮件或运行来历不明的程序；
- 及时更新操作系统及其他应用的高危漏洞安全补丁；
- 定时对重要业务数据进行备份，防止数据破坏或丢失。

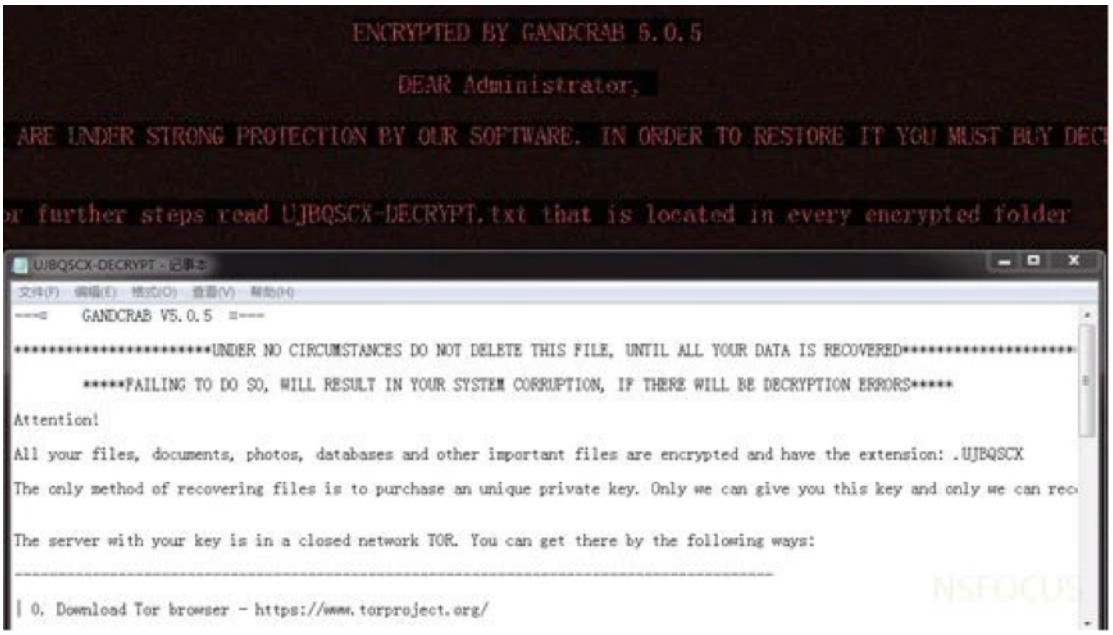
4.1.2 GandCrab 家族

4.1.2.1 背景介绍

GandCrab 勒索病毒于 2018 年 1 月面世以来，短短一年内历经多次版本更新，目前最新的版本为 V5。该病毒利用多种方式对企业网络进行攻击传播，受感染主机上的数据库、文档、图片、压缩包等文件将被加密。若没有相应数据或文件的备份，将会影响业务的正常运行。

从 2018 年 9 月份 V5 版本面世以来，GandCrab 出现了包括了 5.0、5.0.2、5.0.3、5.0.4 以及最新的 5.0.5 多个版本的变种。病毒采用 Salsa20 和 RSA-2048 算法对文件进行加密，并修改文件后缀为 .GDCB、.GRAB、.KRAB 或 5-10 位随机字母，勒索信息文件为 GDCB-DECRYPT.txt、KRAB-DECRYPT.txt、[5-10 随机字母]-DECRYPT.html\txt，并将感染主机桌面背景替换为勒索信息图片。

图 2 GandCrab V5.0.5 桌面截图



4.1.2.2 病毒分析

4.1.2.2.1 传播方式

GandCrab 病毒家族主要通过 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。病毒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并植入该病毒。

4.1.2.2.2 影响范围

Windows 系统

4.1.2.2.3 近期版本变更

5.0 版本：

第一个版本中，需要调用 xpsprint.dll，但该文件在 Windows Vista 和 XP 中不存在，因此无法在上述系统中运行。第二个版本不再使用固定的 .CRAB 或 .KRAB 加密后缀名，而是 5 个字母的随机后缀名。

5.0.1 版本：

此版本修复了一些程序内部错误，但没有进行其他重大更改。

5.0.2 版本：

此版本将随机扩展名长度从 5 个字符更改为 10 个字符，并修复了一些内部错误。

5.0.3 版本：

此版本会通过释放名为 wermgr.exe 的恶意程序来执行加密操作。

5.0.4 版本：

修复了不能在 Windows Vista 和 XP 系统中运行的错误，硬编码了一张人像图片，并在病毒运行时释放到磁盘中。

5.0.5 版本：

更换了加密密钥，以对抗 Bitdefender 等厂商提供的解密工具。

4.1.2.2.4 病毒行为

1. 结束以下进程，其中包括数据库、office 套件、游戏客户端等：

   mysqld.exe、mysqld-nt.exe、mysqld-opt.exe、dbeng50.exe、sqbcoreservice.exe、excel.exe、infopath.exe、msaccess.exe、mspub.exe、onenote.exe、outlook.exe、powerpnt.exe、steam.exe、sqlservr.exe、thebat.exe、thebat64.exe、thunderbird.exe、visio.exe、winword.exe、wordpad.exe

2. 检测键盘布局，对指定语言区域主机不进行加密，如俄罗斯，但不包含中国。
3. 文件加密。
4. 调用系统命令（WMIC.exe shadowcopy delete），从磁盘删除用于备份的卷影副本。
5. 修改当前用户桌面背景为勒索信息图片，其中还包括病毒版本信息。
6. 修改桌面背景后，开始访问指定域名的 80 及 443 端口。
7. 整个加密过程完成后，执行自删除操作。

4.1.2.3 处置方案

GandCrab 在执行完文件加密后会进行自删除，不会驻留系统，也不会添加自启动相关注册表项目。

如文件加密过程还未完成，病毒进程将不会退出，可使用进程管理工具（如 Process Explorer）查看是否有可疑进程，并及时结束，以终止文件加密，减少损失。

4.1.2.4 文件解密

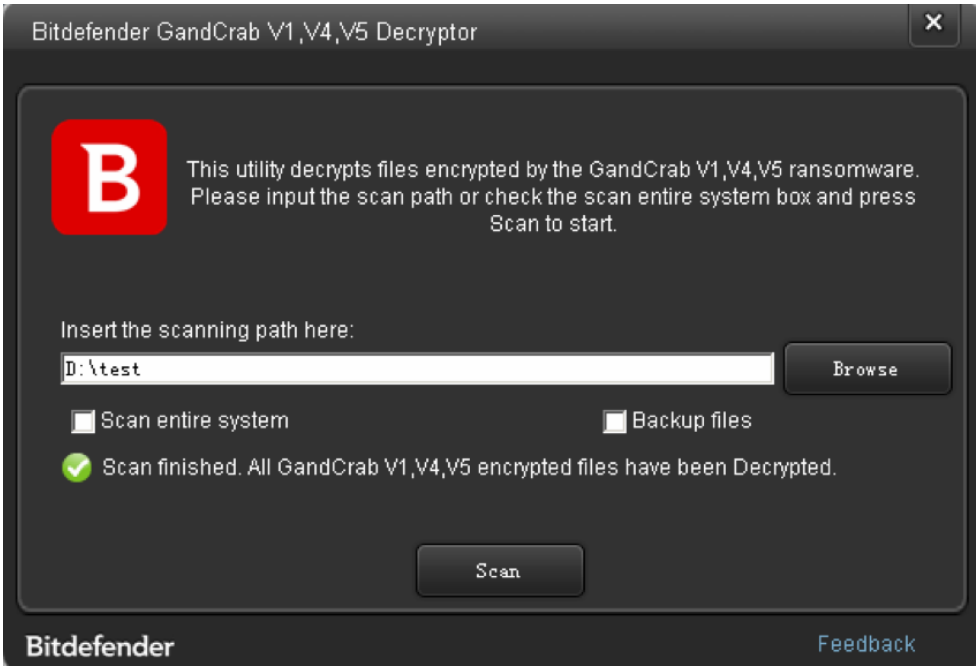
据悉，10 月 16 日，某叙利亚用户在 twitter 上抗议 GandCrab 加密了他的文件，由于无力支付高额赎金，他再也无法看到因战争丧生的小儿子照片，此事件经媒体发酵后，相关黑客对此事做出了道歉，并公布了叙利亚地区之前版本的解密密钥。

解密密钥公开后，多个安全厂商相继发布了解密工具，但为了对抗解密工具，病毒开发者迅速于 10 月 26 日发布了 5.0.5 版本。

10 月 25 日，Bitdefender 发布了解密工具 BDGandCrabDecryptTool，下载地址：https://labs.bitdefender.com/wp-content/uploads/downloads/gandcrab-removal-tool-v1-v4-v5

该工具会通过在线向其服务器提交加密 ID，从而获取可用的解密私钥（ RSA-2048）。经测试，该工具可解密部分 5.0.3 以前版本的加密文件。使用 BDGandCrabDecryptTool 解密 5.0.3 版本加密文件，解密成功。

图 3 GandCrab 解密测试



使用 BDGandCrabDecryptTool 解密最新 5.0.5 版本加密文件，解密失败。

4.1.2.5 专家建议

参考 4.1.1.4 专家建议。

4.1.3 Satan 家族

4.1.3.1 背景介绍

GlobeImposter 和 GandCrab 首次出现的时间分别为 2017 年 11 月和 2018 年 1 月，而 Satan（撒旦）勒索病毒相比于之前的 GlobeImposter 和 GandCrab，可以算得上“历史悠久”。

Satan 最开始出现在 2017 年 1 月份，Satan 病毒的开发者通过网站允许用户生成自己的 Satan 变种，从 2017 年 1 月份到 2018 年 11 月 Satan 病毒一直在持续更新。下表为 Satan 在各个版本中的特点，可以发现 Satan 从最开始单一的勒索病毒逐渐向“蠕虫化”发展。

表 7 Satan 勒索病毒版本变更

版本	V1	V2	V3	V4	V5
首次发现时间	2017 年 1 月	2017 年 12 月	2018 年 5 月	2018 年 6 月	2018 年 11 月
传播特征	RaaS 方式	永恒之蓝	永恒之蓝 JBoss 反序列化漏洞 Jboss 默认配置漏洞 Put 任意文件上传漏洞 Tomcat web 管理后台弱口令 WebLogic WLS 组建漏洞 Apache Struts2 远程代码执行漏洞 Spring Data Commons 远程代码执行漏洞	RaaS 方式 JBoss 反序列化漏洞 Jboss 默认配置漏洞 Put 任意文件上传漏洞 Tomcat web 管理后台弱口令 WebLogic WLS 组建漏洞 Apache Struts2 远程代码执行漏洞 Spring Data Commons 远程代码执行漏洞	永恒之蓝 JBoss 反序列化漏洞 Jboss 默认配置漏洞 Put 任意文件上传漏洞 Tomcat web 管理后台弱口令 WebLogic WLS 组建漏洞 Apache Struts2 远程代码执行漏洞 Spring Data Commons 远程代码执行漏洞 支持在 Windows 和 Linux 平台传播
勒索货币	0.3 个比特币	0.3 个比特币	0.3 个比特币	1 个比特币	1 个比特币
加密后缀	stn	Satan	Satan	dbger	lucky

2018 年 11 月初，绿盟科技发现部分金融客户感染了 Linux 和 Windows 跨平台的蠕虫病毒样本 ft.exe，其采用类似 Satan 勒索病毒的传播渠道，利用多个应用漏洞进行传播。该蠕虫病毒进入系统后无明显破坏行为，仅传播自身。

2018 年 11 月底，国内多个金融客户感染了跨平台的勒索病毒，该病毒是上述蠕虫 ft.exe 的变种版本，病毒会释放门罗币挖矿程序和勒索软件。该勒索病毒可以在 Linux 和 Windows 平台进行蠕虫式传播，并将本地文件加密为 .lucky 后缀，释放勒索信息文件 _How_To_Decrypt_My_File_.Dic。

4.1.3.2 病毒分析

4.1.3.2.1 传播方式

Satan 病毒家族通过下面 10 种通用漏洞进行传播。目前发现 Satan 在 Linux 和 Windows 平台会以 IP 列表 + 端口列表的方式进行漏洞扫描。

1. JBoss 反序列化漏洞

2. JBoss 默认配置漏洞 (CVE-2010-0738)
3. Tomcat 任意文件上传漏洞（CVE-2017-12615）
4. Tomcat web 管理后台弱口令爆破
5. WebLogic 任意文件上传漏洞 (CVE-2018-2894)
6. WebLogic WLS 组件漏洞（CVE-2017-10271）
7. Windows SMB 远程代码执行漏洞 MS17-010
8. Apache Struts2 远程代码执行漏洞 S2-045
9. Apache Struts2 远程代码执行漏洞 S2-057
10. Spring Data Commons 远程代码执行漏洞（CVE-2018-1273）

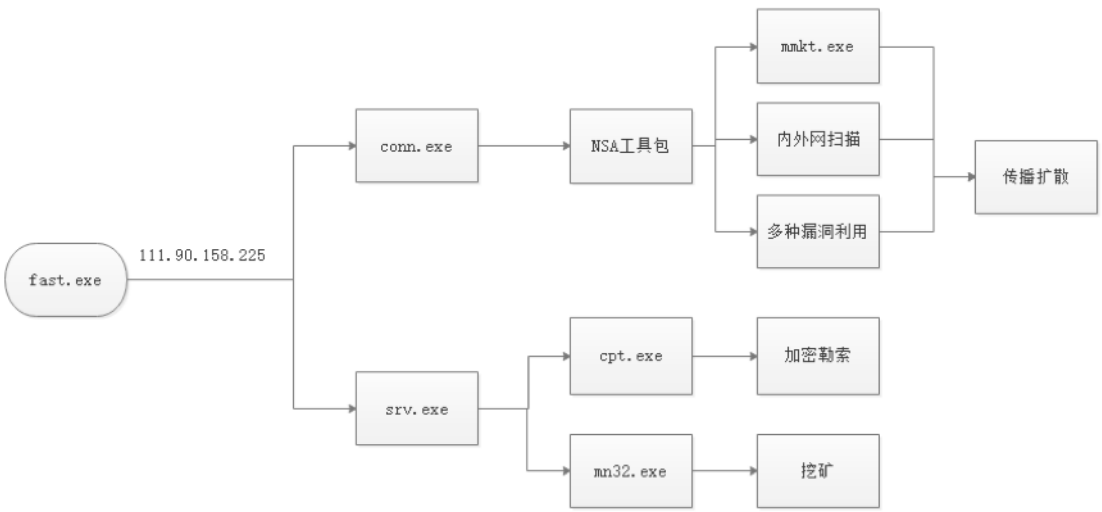
4.1.3.2.2 影响范围

Windows 系统和 Linux 系统

4.1.3.2.3 病毒行为

由于最新版的 Satan 变种病毒攻击流程如下图：

图 4 Satan 勒索病毒传播流程



4.1.3.3 处置方案

Linux

1. 断网隔离防止在木马查杀过程中二次感染。。
2. 检查 crontab 文件和 rc.local 文件，删除 lucky 病毒的相关启动信息。
3. 使用 kill -9 pid 命令结束 .loop、.conn32/64、.cry32/64 进程。
4. 检查 /etc/rc6.d/S20loop 文件指向的位置，删除该目录下相关的样本程序文件，包括 .loop，.conn32/64，.cry32/64，最后删除 /etc/rc6.d/S20loop 文件。
5. 修改操作系统 SSH 服务口令为强口令。

Windows 手动清理

1. 断网隔离防止在木马查杀过程中二次感染。
2. 因为该木马集成弱口令扫描功能以及 mmkt.exe 密码抓取工具，修改系统密码防止在木马查杀过程中二次感染。
3. 结束系统中 blue.exe、fast.exe、star.exe、srv.exe、conn.exe、mmkt.exe 等 6 个进程。
4. 删除 C:\ 目录下的 fast.exe 文件。
5. 删除 C:\Program Files\Common Files\System 目录下的 conn.exe、srv.exe 文件。
6. 删除查看 C:\user\all users 或 C:\ProgramData 目录下的永恒之蓝工具包（根据写入时间判断，避免误删系统正常文件）：
7. 删除木马创建的注册表键值：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Logs Service。
8. 安装针对 MS17-010 漏洞（永恒之蓝利用工具）的操作系统补丁。
9. 修改操作系统密码为强口令。

4.1.3.4 文件解密

在获知其加密算法及密钥前提下，即可对加密文件进行解密，绿盟科技西安网络攻防实验室为此编写了解密工具，测试适用于 v2 至 v4 版本，并支持文件名还原及批量文件解密。

使用说明：

1. 直接在当前目录双击运行，即可解密该目录下相关加密文件
2. 解密完成后，将自动恢复原文件名，并保留原加密文件
3. 程序默认只遍历三级子目录，如目录数大于三级，可通过命令行指定
4. 命令行下支持目录及遍历层数两个参数，如：decrypt.exe D:\test 5

图 5 Satan 勒索病毒解密测试

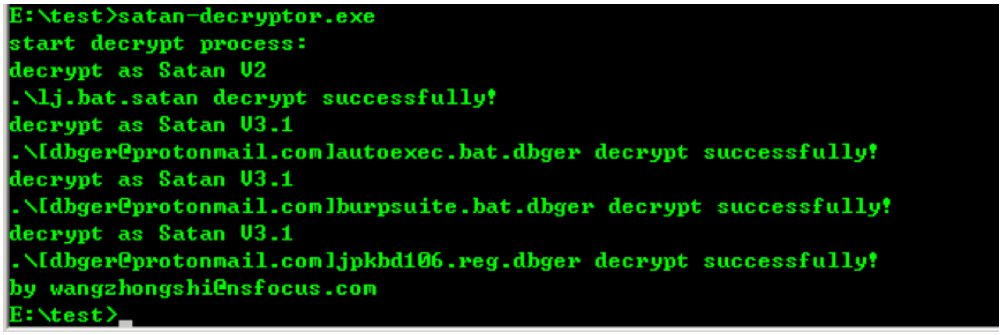
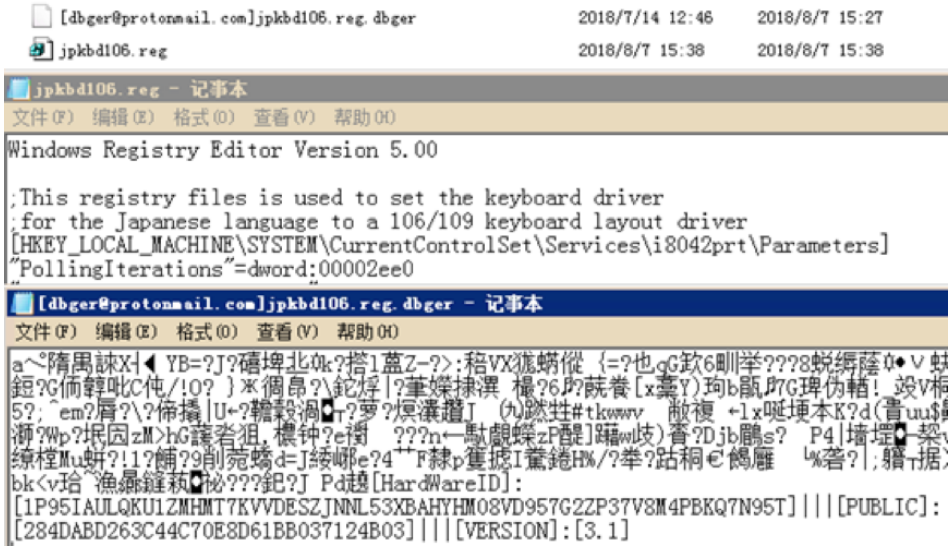


图 6 .debger 文件解密成功



4.1.3.5 专家建议

- 更新 Apache Structs2 组件版本到最新，修复 (s2-045)(s2-046)(s2-057) 漏洞；
- 更新 JBoss 版本到最新，修复 (CVE-2013-4810) (CVE-2010-0738) 漏洞；
- 更新 Tomcat 修复任意文件上传漏洞 (CVE-2017-12615)；
- 更新 WebLogic 版本修复任意文件上传漏洞 (CVE-2018-2894) 和 WLS 组件漏洞 (CVE-2017-10271)；
- 更新系统补丁，修复 MS17-010 漏洞，或者关闭不必要的 SMB 服务。
- 加强主机账户口令复杂度及修改周期管理，并尽量避免出现通用或规律口令的情况；
- 修改系统管理员默认用户名，避免使用 admin、administrator、test 等常见用户名；
- 安装具备自保护的防病毒软件，防止被黑客退出或结束进程，并及时更新病毒库；
- 加强企业员工安全意识培训，不轻易打开陌生邮件或运行来历不明的程序；
- 及时更新操作系统及其他应用的高危漏洞安全补丁；
- 定时对重要业务数据进行备份，防止数据破坏或丢失。
- 不同业务网络之间做好 VLAN 或端口隔离，防止病毒在内部跨网段传播。
- 关注漏洞预警信息，及时修复重要漏洞，如绿盟科技安全预警公众号。

4.2 挖矿事件典型案例

4.2.1 利用 WebLogic 组件漏洞挖矿

4.2.1.1 背景介绍

2018 年初，绿盟科技应急响应团队持续接到来自金融、卫生、教育等多个行业客户的安全事件反馈，发现多台不同版本 WebLogic 主机均被植入了相同的恶意程序，该程序会消耗大量的主机 CPU 资源。经过对捕获到的攻击代码进行分析，发现这是一次针对 WebLogic 的 wls-wsat 组件漏洞（CVE-2017-10271）进行远程代码执行的大范围攻击。

4.2.1.2 处置过程

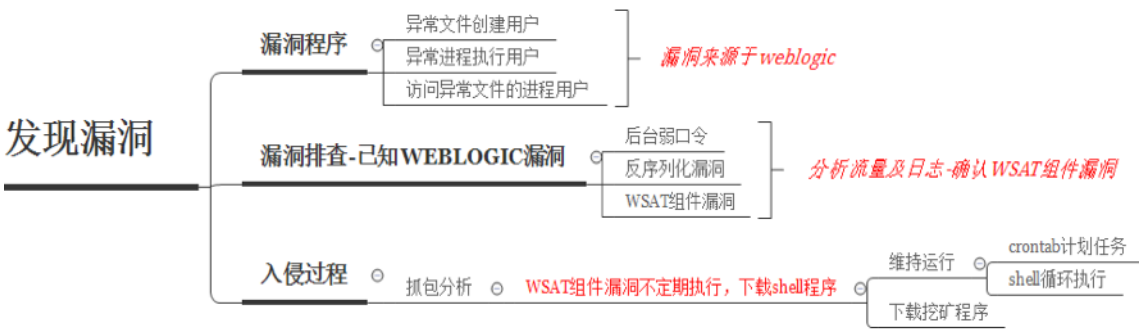
被感染主机 tmp 目录下均存在可执行文件 watch-smartd 或 Carbon，通过分析上述文件均为不同版本的虚拟币挖矿程序 cpuminer，因此运行后会大量消耗服务器 CPU 及内存资源；该挖矿程序不存在维持进程和复活功能，但在清除后又会不定期出现。

收集信息得知挖矿程序的所属用户和运行用户与 WebLogic 的运行用户相同。查看发现 watch-smartd 进程的父进程为 WebLogic。由此可以确定该事件与 WebLogic 漏洞有关。

通过对感染主机抓包捕获攻击代码以及 WebLogic 日志分析，证实攻击者是利用 WebLogic wls-wsat 组件远程代码执行漏洞（CVE-2017-10271）下载并运行挖矿程序。

排查过程可参考下图：

图 7 入侵过程



首先攻击者通过该漏洞执行 curl 命令，下载名为 setup-watch 的 shell 脚本，其作用为下载并运行最终的挖矿程序。该 shell 脚本中定义了挖矿程序的下载地址、下载方式、保存路径、运行参数等。

通过对服务器上的样本程序进行分析，绿盟安全人员发现 watch-smartd 或 Carbon 为同一挖矿程序程序的不同版本。攻击者主要利用该程序挖取在黑市流通的 XMR（门罗币），其对外连接的矿池域名为：minexmr.com、minergate.com。

4.2.1.3 处置方案

从主机层面可通过监控主机系统资源或进程分析方式进行检测，从网络层面可对 C&C 地址及矿池相关域名 /IP 进行监控，以发现其他受感染主机。

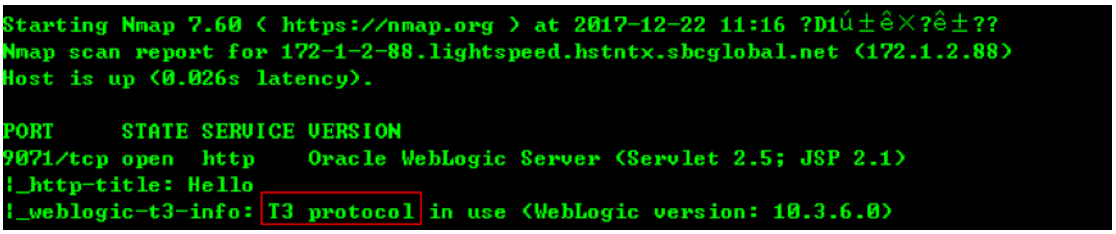
针对 Linux 主机，首先查看 /tmp 目录中是否存在属主为 WebLogic 运行账户的相关可疑文件，如：watch-smartd、Carbon、default。

通过进程及系统资源分析，确认是否存在启动用户为 WebLogic 运行的相关可疑进程。

漏洞修复及验证：

1. 首先在网络中通过端口探测方式，检测对外开放了 T3 协议的 WebLogic 主机，若非业务需要，可通过网络边界设备对相应端口进行封禁。

图 8 检测 T3 协议



2. 安装 Oracle 官方提供的 WebLogic 2017 年 10 月份补丁，漏洞通告及相关补丁参考链接：http://www.oracle.com/technetwork/security-advisory/cpuoct2017verbose-3236627.html

3. 若无法安装上述补丁，还可根据主机实际环境，删除或重命名 WebLogic 目录中以下 war 包及目录。

/home/WebLogic/Oracle/Middleware/wlserver_10.3/server/lib/wls-wsat.war

/home/WebLogic/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/.internal/wls-wsat.war

/home/WebLogic/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/wls-wsat

重启 WebLogic 后，通过 console 端口（T3 协议）访问 wls-wsat，验证响应状态码是否为 404。

4.2.1.4 专家分析

此次攻击主要目的为下载并执行挖矿程序。尽管该漏洞早已在 Oracle 官方发布的 2017 年 10 月份

的补丁中修复，即安装了最新补丁的主机将不受此次攻击影响，但还是存在大量的主机被入侵。这表明很多企业对于网络安全建设的长期忽视，对已知高风险漏洞的不重视，才会大量爆发 WebLogic 挖矿事件而付出惨痛代价。漏洞一旦存在，就随时可能被不法分子利用，甚至会导致重大资产的损失和承担法律责任。

目前黑色产业链中利用已知 1Day 或 NDay 攻击服务器，谋取利益的事件越来越多。企业应该重视并全面提升自身系统的安全性，从而保障业务顺畅运行，也保护用户信息安全。

4.2.1.5 专家建议

1. 企业需要重视自身安全制度的建设，与专业安全厂商建立合作机制，共同抵御网络攻击，保证企业自身业务的正常运行。
2. 建设完善的企业安全管理规范，及时更新补丁，尤其在重大安全漏洞公布时，及时更新并确定所有相关服务器更新成功。防微杜渐，防患于未然。

4.2.2 WannaMine 及其变种

4.2.2.1 背景介绍

2018 年，绿盟科技应急响应团队持续接到 WannaMine 挖矿的事件反馈。该蠕虫感染计算机后会向计算机中植入挖矿病毒，导致电脑资源被大量占用，无法正常运行，危害巨大。但至今仍有大量主机未安装安全补丁，导致被后续的 Wanna 系列变种病毒感染。

2018 年 3 月，WannaCry 勒索病毒出现变种，WannaMine 挖矿病毒诞生。

2018 年 5 月，WannaMine 出现变种（WannaMine2.0）。

2018 年 11 月，WannaMine2.0 再次出现变种（WannaMine 3.0）。

在局域网内，WannaMine 家族利用 SMB 协议漏洞，快速横向扩散。WannaMine 家族 2.0、3.0 变种，加入了一些免杀技术，传播机制与 WannaCry 勒索病毒一致。

4.2.2.2 处理过程

WannaMine 病毒使用“永恒之蓝”漏洞入侵服务器，然后植入挖矿程序，并扫描同网段主机传播漏洞。特征图如下：

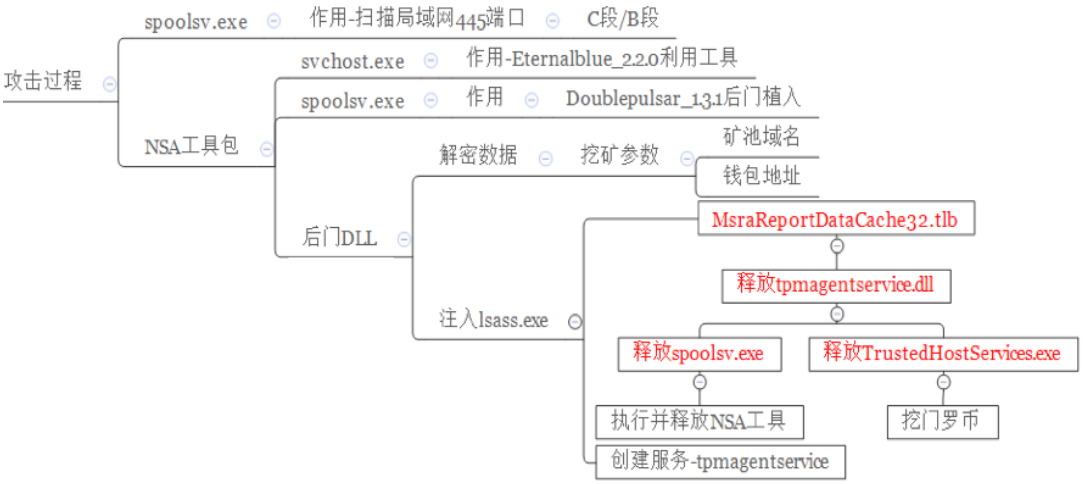
图 9：病毒特征

WannaMine 病毒攻击传播过程：

1. srv（tpmagentservice.dll）主服务，开机启动，加载 spoolsv。
2. spoolsv（spoolsv.exe）对局域网进行 445 端口扫描，确定可攻击的内网主机。同时启动挖矿程序 hash（TrueServiceHost.exe）、漏洞攻击程序 svchost.exe 和 spoolsv.exe（NSA 工具包）。
3. svchost.exe 执行“永恒之蓝”漏洞溢出攻击（目的 IP 由第 2 步确认），成功后 spoolsv.exe(NSA 黑客工具包 DoublePulsar 后门）安装后门，加载后门 dll。
4. 后门 dll（x86.dll、x64.dll）执行后，负责将 MsraReportDataCache32.tlb 从本地复制到目的 IP 主机，再解压该文件，注册 srv 主服务，启动 spoolsv 执行攻击。

WannaMine 病毒每攻陷一台服务器，都将重复以上步骤。攻击过程如下图：

图 10：攻击过程



事件排查—网络层：

通过出口防火墙或其他类似安全设备，对相关的后门域名、挖矿域名及 Kill Switch 域名（www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com）请求进行监测，以发现内部其他感染主机。

部分域名信息如下：

表 8 部分域名信息

序号	域名	域名解析地址
1	swt.njaavfxcgk3.club	31.0.0.0
2	tar.kziu0tpofwf.club	127.0.0.1
3	rer.njaavfxcgk3.club	127.0.0.1
4	acs.njaavfxcgk3.club	127.0.0.1
5	nicehash.com	104.17.60.220
6	p3.qsd2xjpzfky.site	179.61.233.32
7	p1.mdfr6avyyle.online	136.243.102.157
8	p1.qsd2xjpzfky.site	179.61.233.32
9	p5.qsd2xjpzfky.site	179.61.233.32

事件排查—主机层：

1. 检查主机是否存在以下进程：

   TrustedHostServices.exe（WannaMine1.0-2.0 门罗币挖矿程序）

   trustedhostex.exe（WannaMine3.0 门罗币挖矿程序）

   Spoolsv.exe（有 445 端口扫描行为）

2. 检查主机是否存在以下服务：

   Tpmagentservice（WannaMine1.0 服务）

   wmassrv（WannaMine2.0 服务）

   snmpstorsrv（WannaMine3.0 服务）

3. 检查主机中是否存在以下目录或文件 :

   WannaMine1.0 目录：

   - C:\Windows\SecureBootThemes

- C:\Windows\System32\SecureBootThemes

WannaMine2.0 目录：

- C:\Windows\SpeechsTracing

WannaMine3.0 目录：

- C:\Windows\appdiagnostics

4. 相关文件包括：

C:\Windows\system32\tpmagentservice.dll（WannaMine1.0 相关）

C:\Windows\system32\TrustedHostServices.exe（WannaMine1.0 相关）

C:\Windows\System32\MsraReportDataCache32.tlb（WannaMine1.0 相关）

C:\Windows\system32\wmassrv.dll（WannaMine2.0 相关）

C:\Windows\system32\EnrollCertXaml.dll（WannaMine2.0 相关）

C:\Windows\system32\HalPluginsServices.dll（WannaMine2.0 相关）

C:\Windows\system32\snmpstorsrv.dll（WannaMine3.0 相关）

C:\Windows\system32\trustedhostex.exe（WannaMine3.0 相关）

C:\Windows\system32\marstracediagnostics.xml（WannaMine3.0 相关）

4.2.2.3 处置方案

从主机层面可通过监控主机系统资源或进程分析方式进行检测。

从网络层面可对 C&C 地址及矿池相关域名 /IP 进行监控，以发现其他受感染主机。

漏洞修复及病毒清理：

手动清理

1. 禁用并删除相关后门服务，包括：tpmagentservice、wmassrv、snmpstorsrv；
2. 删除上述服务对应执行文件及其他相关的释放文件；

清理脚本

针对 Wanna 系列病毒，可以使用绿盟科技 WannaMine 清理脚本进行清理。

4.2.2.4 专家分析

微软官方在 2017 年 3 月 14 日公布了 MS17-010 的安全公告，但如今 Wanna 系列勒索、挖矿蠕虫病毒入侵事件仍然在各大行业时有发生。这说明企业对于已知漏洞攻击还抱有侥幸心理或者安全意识不足，认为一段时间之后不会发生此类安全事件，放松警惕；然而漏洞一旦存在，就随时可能被不法分子利用，甚至会出现变种病毒或者其他新的利用方式。

目前利用已知 1Day 或 NDay 攻击服务器、谋取非法利益的事件越来越多，主要利用方式有数据窃取，勒索，挖矿，发起 DDoS 攻击等。企业应该重视并全面提升自身系统的安全性，从而保障业务顺畅运行，也保护用户信息安全。

4.2.2.5 专家建议

1. 企业网络建设中应该进行安全域的划分；办公网、生产网，区域网之间应进行严格的区分隔离。
2. 服务器应启用防火墙，关闭不必要的端口。
3. 建设完善的终端安全管理规范，及时更新系统补丁，尤其在重大安全漏洞公布时，及时更新并确定所有主机更新成功。防微杜渐，防患于未然。

4.3 入侵事件典型案例

4.3.1 某网站博彩暗链事件

4.3.1.1 背景介绍

2018 年 10 月初，工作人员发现 WAF 设备告警拦截到大批量“博彩”页面。系统为一款商业应用软件 TRS，应用架构：一台后台制作服务器，前台两台发布服务器，一主一备。编辑人员从后台系统发布新闻生成静态页面，通过同步进程将文章同步到前台一主一备服务器上。分析发现前台两台服务器存在的博彩文件完全相同。

4.3.1.2 处理过程

纵向对比正常的 HTML 文件，前后台服务器的 HTML 文件是一致的。因此，初步判断入口可能在后台服务器上。

后台服务器 WebShell 排查

对后台的 Web 目录进行扫描，发现存在三个 WebShell 大马，分别是：

- /wcm/js/yjh.jsp
- /wcm/logo/yjh.jsp
- /wcm/WCMV6/editor/editor/index.jsp

分析文件最后修改时间为 2018 年 7 月 22 日。

/wcm/logo/yjh.jsp 文件为 WebShell 大马，密码为：admin。该木马具备文件创建、删除等功能。

图 11 WebShell 大马

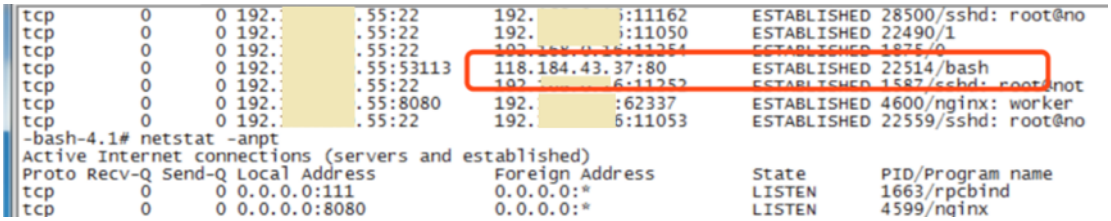
直接访问 WebShell：http://****/wcm/logo/yjh.jsp，弹窗提示需要进行登录，因此可确定攻击者得到了后台登陆账号和密码，授权后访问的 WebShell。通过后台管理员账号登陆后再次访问，木马成功利用。

分析后台登陆日志，发现只有最近一段时间的日志记录，无法判断事发时登陆用户。

后台服务器后门排查

继续排查服务器是否存在恶意进程，排查过程中，发现一个可疑的连接：

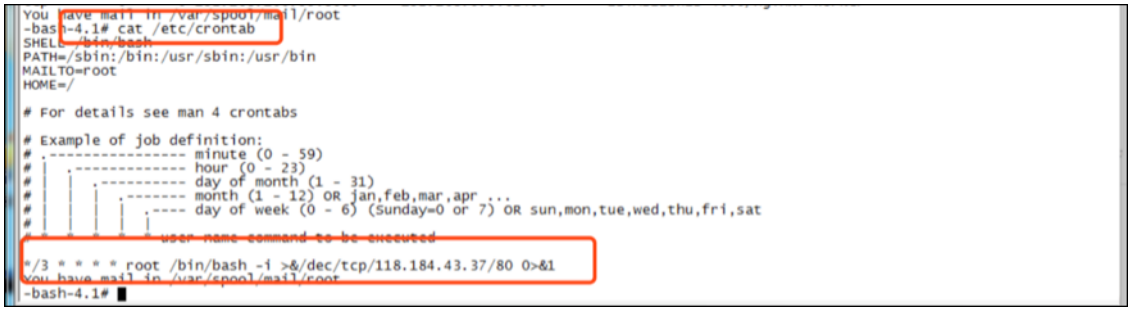
图 12 可疑连接



服务器主动连接 118.184.43.37 的 80 端口（该 IP 来自香港）

工作人员分析疑似为 SSH 后台，于是进行服务器“计划任务”检查，发现存在一个定时任务。

图 13 发现定时任务



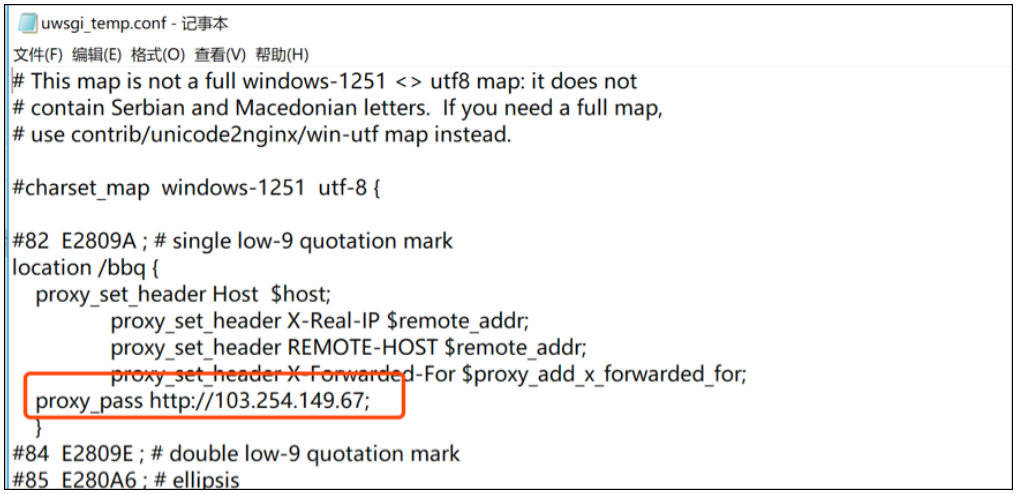
该任务的作用是定期将 SSH 会话反弹到目标服务器 80 端口，从而实现在没有 SSH 口令的状态下登陆服务器。

前台服务器检查

从工作人员那了解到所有的密码一致，因此存在从后台服务器入侵后再 SSH 连接到前台服务器，利用后台服务器的密码直接登陆的可能。因为服务器没有运维审计系统，因此历史的登陆及操作日志都无法记录。

并且从系统运维人员那边得知，发现配置文件被修改。前台服务器的 nginx 文件夹下多出一个配置文件。

图 14 可疑配置文件

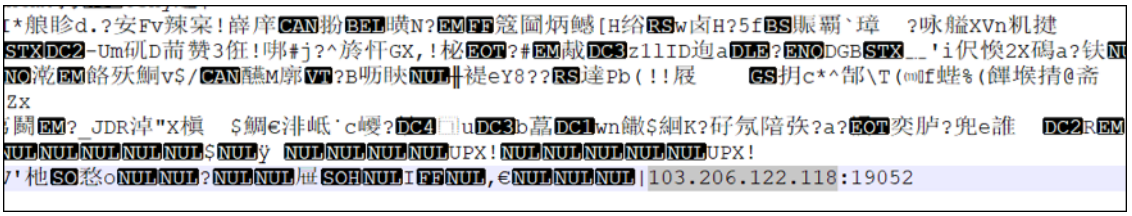


proxy_pass http://103.254.149.67 的功能为路径重定向，这也是导致绿盟科技发现 WAF 上有拦截敏感字眼但是在服务器上找不到 HTML 文件的原因，对比下面两个 URL。

纵向对比前台主服务器 192.***.***.51 与备服务器 192.***.***.81，发现主服务器被创建的配置文件在备服务器上并没有。因此基本可以判断主服务器 192.***.***.51 也被入侵，可能也被植入后门。

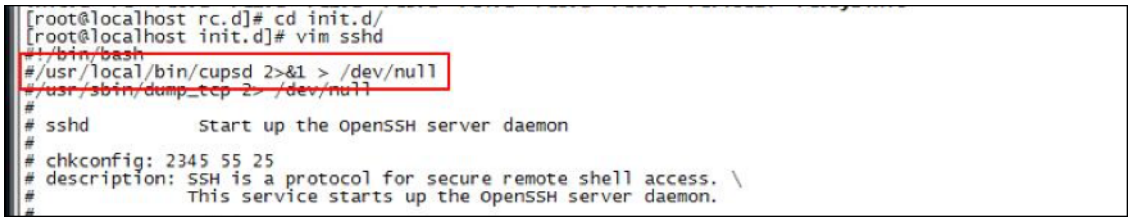
查看 /usr/local/bin/cupsd 文件，发现存在同样一处后门：

图 15 后门



同样 IP 来自香港（103.206.122.118），并且存在反弹 shell：

图 16 反弹 shell



攻击者利用这些 shell，可以远程控制服务器。查看博彩 HTML 页面，发现主体为正常页面，标题及部分字眼被修改过。因此判断可能被在服务器上执行批量脚本。

4.3.1.3 专家分析

1. 攻击者通过管理后台功能上传 WebShell，并且成功利用 WebShell。
2. 攻击者利用 WebShell 在后台服务器上创建后门，达到监听 22 端口的效果。
3. 通过端口监听机制获取服务器密码，利用前后台服务器密码一致成功登陆前台服务器。
4. 攻击者同样在前台服务器上留下后门，反弹 shell 进行服务器控制。
5. 通过控制服务器达到执行脚本从而进行批量篡改静态文件的目的。

4.3.1.4 专家建议

1. 因为前台服务器还残留博彩页面，因此需要技术人员将后台服务器的静态 HTML 文件覆盖到前台服务器。
2. 服务器密码严格进行把控，做到“一机一密”，“一月一密”，服务器密码单独设置，复杂度要求要，更换频率高。
3. 加强服务器运维审计建设，对运维人员、工作人员的运维进行审计及控制，出问题可以进行回溯。
4. 后台管理系统严禁部署于互联网上。
5. 加强后台管理系统双因素认证，采取“密码 +CA” “密码 + 指纹” “密码 + 短信”等形式。
6. 对服务器权限进行严格控制，外访内采用精确到端口级别的访问控制策略，内访外精确到 IP 级别或者端口级别的访问控制策略。
7. 加强日志管理，要求所有日志满足 180 天以上的存储要求。

附录 A: 绿盟应急响应服务介绍

应急响应是一项对技术专业性要求很高、经验依赖性很强的工作。需要应急人员掌握足够的基础知识，包括：操作系统、数据库、网络设备等，以及必要安全技能，如：常见攻击入侵途径、流行攻击手段等，同时还需具备一定的追踪溯源及沟通协调能力。

绿盟科技具备一支常年研究安全技术、实时跟踪安全动态的专业应急响应团队，对分析处置各种流行安全漏洞和安全事件均有成熟的分析方法和丰富的处置经验，可面向客户提供从事件判断到事件处置以及事件总结的完整应急服务。

具体的服务模块包括：事件预警、后门提取、样本分析、日志分析、数据恢复、隐患排查、攻击溯源、攻击还原、应急演练、应急培训、体系建设以及解决方案，相关服务项概述如下：

表 9 应急响应服务项概述

服务项	服务概述
普通事件响应	传统安全事件响应，包括：普通 web 入侵、主机入侵、病毒木马、DDoS 攻击等
重大事件响应	涉及具体业务或重大入侵安全事件，如：信息泄密、业务损失、APT 攻击等
后门提取	对系统或应用中的后门进行排查提取，如：病毒木马、系统后门、WebShell 脚本等
样本分析	对捕获的样本进行动态与静态分析，包括：X86、ARM、MIPS 等多平台样本
日志分析	对日志进行数据分析，如：web 日志、操作系统日志、应用日志、设备相关日志等
攻击溯源	对事件中涉及攻击者进行溯源，包括：IP 地址、地理位置、个人信息等
应急响应培训	为企业安全团队或运维相关技术人员提供具体的应急响应技术培训
应急响应演练	提供相关安全事件场景的应急响应演练服务，包括：方案设计、环境搭建等
安全解决方案	针对公开的典型安全事件或者已经发生的安全事件提供有效的解决方案
应急响应体系建设	为企业应急响应体系以及应急管理流程提供咨询或整体建设方案

同时根据不同安全事件的处置需求，还推出了应急响应服务包，包括：黄金服务包、白金服务包以及钻石服务包，不同服务包在应急服务模块上有所差异，其中钻石服务包涵盖所有模块。

附录

图 17 应急响应服务包

应急响应服务包		黄金服务包	白金服务包	钻石服务包
服务模块	后门提取	✓	✓	✓
	攻击还原	✓	✓	✓
	事件预警	✓	✓	✓
	日志分析	✗	✓	✓
	隐患排查	✗	✓	✓
	样本分析	✗	✗	✓
	攻击溯源	✗	✗	✓

附录 B: 绿盟安全预警公众号介绍

面对突发的高危事件，绿盟科技安全预警将会发布包含解决方案的处置手册，快速提供针对新威胁的检测和防护方案，结合人工排查、临时防护和产品防护，将处置方案实际落地客户现场。同时，我们还会提供安全加固和技术分析资料，协助客户提升安全能力。

图 18 绿盟科技安全预警公众号

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