深度

评论

# WhatsApp是如何被利用来监控异见人士的?

应该承认，在现在这个时代，并不存在既方便又有效的隐私保护方法。

乐之 | 2019-11-27

西班牙一个示威中，示威者使用手机拍摄。摄：Pau Barrena/AFP via Getty Images

10月29日，WhatsApp和Facebook联合起诉以色列入侵技术提供商NSO Group及其母公司Q Cyber，称被告“逆向工程”了WhatsApp的客户端和通讯协议、非法使用WhatsApp服务器，利用WhatsApp的漏洞，将木马植入约1400台设备，目标用户有律师、记者、人权活动家、异见者、外交官和外国政府官员。

这不是NSO第一次被告了。去年10月，华盛顿邮报记者Jamal Khashoggi被杀，两个月后，沙特阿拉伯异议人士Omar Abdulaziz起诉了NSO，称NSO在他的手机上安装木马软件，用于为沙特阿拉伯王室监控Khashoggi与他的通讯。也是去年12月，NGO国际特赦组织也向以色列国防部提过要求，希望以色列取消NSO的国防出口执照，因为NSO的软件用于监控一位国际特赦组织的员工。

## 致命漏洞

> 利用NSO的木马程序的监控者分布在45个国家或地区，集中在中东、南北美洲、欧洲、南亚等地，非洲、东南亚、中亚、东亚等也偶有发现。

几份起诉书异口同声，说NSO植入的木马是“Pegasus”。据网上流传的Pegasus宣传册，这一木马专为远程隐蔽监控设计，兼容iOS、Android、Blackberry，植入智能手机之后，可以截取短信、电话通讯，也可以从WhatsApp、Skype等第三方软件中提取通讯记录，还可以操控电话麦克风、照相机，从GPS系统搜集信息，亦可调取日历、电邮、浏览记录等数据。

可以说，植入这一木马之后，这台手机就在无时无刻、无声无息地为入侵者监控其持有者。Pegasus系统包括两个部分：木马客户端和后台服务器。木马客户端植入攻击对象的电话，后台服务器则负责接收和存储木马发送过来的监控信息，也可以向客户端发送指令，甚至远程升级木马。

起诉书点了两个漏洞的名：CVE-2016-4657和CVE-2019-3568。

第一个漏洞，2016年由Citizen Lab和Lookout联手披露，其实不是WhatsApp的漏洞，而是苹果iOS浏览器Safari的漏洞：黑客可以构造携带恶意代码的网页，一旦用户用Safari打开这个网页，网页可以在iOS操作系统上运行任意代码。

根据Lookout当时的报告，NSO炮制了“三叉戟”攻击，就是同时用了三个漏洞，先执行恶意代码，然后确定iOS内核在内存中的位置，最后修改内存获取操作系统“根用户”权限（也就是俗称的“越狱”）。此后，植入NSO的木马Pegasus，即可对手机全面监控。

在入侵过程中，WhatsApp只是扮演传送恶意网页链接的角色。这个恶意链接，就算用微信、Telegram发过去，只要用户点了，也都会有效。

第二个漏洞，就确实是WhatsApp的问题了，影响也更严重。简而言之，通过这个漏洞，入侵者可以向WhatsApp发送特制的数据包，内含恶意代码，让WhatsApp以为收到视频来电，然后用户甚至不需要接听，就可以通过WhatsApp的客户端执行恶意代码。不止iOS，Android系统也可以攻击，甚至照顾到了小众系统如微软的Windows Phone和基于Linux的Tizen。

WhatsApp今年5月修好了这个漏洞，在起诉书中，WhatsApp说被告的员工跟人抱怨WhatsApp把漏洞修好了，还弄得人尽皆知。

这两条入侵路径都不需要在物理上接触用户的手机，第一条路径需要用户点击网页链接，第二条不需要用户做任何操作。

2018年，Citizen Lab发了一份跟进报告。他们利用2016年截取的Pegasus木马，获取了一份疑似Pegasus后台服务器名单；然后再根据这些服务器的行为，形成一个“服务器指纹”；然后再用这些服务器指纹扫描互联网上的其他服务器，检索其他有可能是Pegasus后台的服务器。之后，再用这些后台服务器地址，逆向检索向这些服务器发送消息的客户端，从而摸索出有哪些机器被Pegasus植入了。

根据这份报告，Pegasus的用户（监控者）分布在45个国家或地区，集中在中东、南北美洲、欧洲、南亚等地，非洲、东南亚、中亚、东亚等也偶有发现，其中10个监控者执行“跨

境监控”，例如在美国国外监控在美国的人。Citizen Lab没有研究中国大陆的流量，但是香港有木马感染的案例检出（该监控者同时也监控印度、巴基斯坦、孟加拉和巴西的用户，不像是针对香港，香港的感染或许是被监控者旅行到香港时录得）。

Facebook 及 Whatsapp 总裁扎克伯格 (Mark Zuckerberg)。摄：Zach Gibson/Getty Images

> 若手机遭受Pegasus植入，端到端加密也没有用。

虽然说WhatsApp实现了“端到端加密”，就是说，用WhatsApp的两个人，他们的客户端会各自生成加密密钥并交换，此后发送给对方的消息会用对方的密钥加密，这样只有对方才能解密、阅读通讯内容，即使是WhatsApp官方也看不到，互联网中间节点也只能看到加密后的消息，无法直接阅读内容。

但若手机遭受Pegasus植入，端到端加密也没有用，因为Pegasus攻击目标不是密文，甚至不是通讯软件本身，而是支持通讯软件运作的操作系统。

操作系统比通讯软件更底层：通讯软件加密所需要的所有信息和运算资源，都是由操作系统提供的；通讯软件解密后的信息，也需要通过操作系统向用户呈现。操作系统知道用户在屏幕键盘上点击了哪些键，也知道通讯软件要显示的文字内容是什么，所以，一旦木马获取了操作系统的控制权限，通讯软件就几乎没有办法保护自身信息安全。

## 漏洞为何会出现

> 究其根本，原因是智能手机其实是一台计算机，而计算机，原本是用来算数的。今天我们用智能手机和电脑做的事情，大大偏离了“计算机”原始的设计目标。

WhatsApp是2009年成立的，2014年Facebook以190亿美元收购。Facebook全球有三万余员工，现金流稳定增长，给技术人员开出的价码也是行业顶尖。

苹果开发操作系统，经验非常丰富：iOS的核心Darwin，可以追溯到1989年的NeXTSTEP（乔布斯被苹果开除后自立门户开发，后来又被苹果收购回去），NeXTSTEP又可以追溯到70年代的UNIX系统。库克近几年也不断以“隐私”为苹果生态体系的买点。

可以说，Facebook和苹果都有人才、有经验、有动力也有钱去完善信息安全，为什么它们还是不断爆出漏洞，让NSO这样以入侵系统为业的企业有生存空间呢？

究其根本，原因是智能手机其实是一台计算机，而计算机，原本是用来算数的。今天我们用智能手机和电脑做的事情，大大偏离了“计算机”原始的设计目标。

现代可编程计算机，理论源头是图灵的“图灵机”。图灵机是一台抽象的机器，有一条“磁带”和一个“磁头”，磁带分为一个个格子，格子可以填写数字或者指令，磁头可以对格子读取或者写入，或者执行格子里面的命令。纸带对应我们今天的“内存”，读写头对应我们今天的CPU。

如果“计算机”只是停留在“算数”的功能上，它的“问题率”其实非常低：现代的CPU的“计算”功能极少出错，上一回应该是1994年Intel奔腾芯片的FDIV问题，这些CPU在计算某些罕见的小数除法的时候，会算错数。

但是我们想要的是“电脑”，不是“计算机”。我们想要上网、看视频、记笔记、玩游戏、发电邮。

为此，业界发明了各种编程语言和编译器，从而软件工程师不用手写CPU的指令，而是可以在用多少近似于人类语言的编程语言给电脑下指令。又为了让CPU能使用各式显示器、网卡、播放声音，软件工程师又写了各式驱动程序，从而让CPU能够将数字转化为图像、声音和通讯信号。CPU上被架了一层“操作系统”，从而程序的开发者不用为每一种计算机开发程序；为了让多个程序同时运行，比如播放音乐的时候显示网页，人们又开发了“多任务”操作系统。

问题是，电脑架构一路走来，在硬件层面，几乎还是那个简单的“一块内存，一个CPU”的模型。尽管我们后来加入了“程序不能干涉操作系统核心的运作”、“用户不能读取其他用户的数据”等等的逻辑，对于CPU来说，它还是能够读写所有的内存。几乎所有的权限限制，都是在软件层面实现的，如果编写者不小心留下漏洞，那入侵者就可以想办法“骗”CPU去为他们读取或者篡改数据。

## 开源也不一定安全

> 其一，开源软件的维护很多人都是志愿者在做，免费为项目共享代码；我们用户又不给钱，也很难在道义上要求开源开发者做到怎样的标准。其二，有些巨大漏洞在代码上，就是漏了几行边界检查的代码，是很常见又难以检查出的错误。

有人会说，WhatsApp是闭源的，苹果系统也有大量闭源组件，而且在iOS上强制所有浏览器使用Safari的Webkit内核，只要我们用公开透明的开源软件，全世界的技术专家一起来审查代码，那就会安全了。

这恐怕不切实际，因为开源软件一样有过影响极其恶劣的漏洞。

2014年，开源加密库OpenSSL爆出“Heartbleed”（中文称“心脏出血”）漏洞，用密码学大师Bruce Schneier的话说，“从1到10，这（Heartbleed的严重程度）是11”。

OpenSSL是什么呢？简而言之，OpenSSL是一个开源的SSL实现（注），而SSL可以给浏览器（如Mozilla Firefox、Google Chrome等）和网站服务器（如google.com、facebook.com等）之间的通讯提供“端到端加密”，从而免受互联网中间节点窥探、篡改。网站运营商可以免费用这个软件，给自己的网站服务器加上SSL，从而让传输变得安全，不会泄露用户隐私数据，如密码、信用卡号等等。当时，OpenSSL的用户有维基百科、雅虎、社交媒体Reddit、Tumblr，交易平台Stripe等等。

问题是，如果这个提供安全的软件本身不安全怎么办？2011年12月31日，一位OpenSSL的开发人员给项目提交代码，实现SSL的“心跳”功能，结果引入了一个漏洞，导致数据泄漏，故称“心脏出血”。

OpenSSL是万维网服务器软件Apache和nginx的基础，这两个软件也是开源软件，但他们的维护者也没有发现OpenSSL的漏洞。于是，如果网站服务器用了有Heartbleed漏洞的服务器软件（当时Apache和nginx市场占有率合计66%），这台服务器就可能直接泄漏其他

用户的数据，只要服务器软件曾经收发过这些数据，甚至可能泄漏服务器端的加密私钥，从而让攻击者解密用户和服务器的加密通讯，让SSL提供的安全性荡然无存。

分布式网络服务Tor（洋葱路由）干脆发了篇文章说，如果你很在乎匿名和隐私，未来几天就不要上网了（等大家把服务器漏洞补好再回来）。

Heartbleed漏洞从引入到发现，花了两年时间。期间，使用了有漏洞的OpenSSL的服务器，在网站运营者自以为启用端到端加密保证传输安全的同时，不知道泄露了多少用户数据出去。

可是这也不能怪开源项目开发者。其一，他们很多人都是志愿者，免费为项目共享代码；我们用户又不给钱，也很难在道义上要求开源开发者做到怎样的标准。其二，这个漏洞在代码上，就是漏了几行边界检查的代码，这样的错误对于程序员来说是非常常见的，也很难查，提交的时候没审到，之后就很难再发现了。

群众正在使用手机拍摄。摄：Giuseppe Cacage/ AFP via Getty Images

## “互联网思维”的问题

追求极速迭代而造成的种种失误。

Facebook有句口号，叫做“Move fast and break things”，就是说要快速迭代，推出新功能；别怕写出问题，有问题修就是了。Facebook从2004年创办，8年内做到上市，如今市值5500亿美元，这个思路或许确实有可取之处吧。

不知道是不是受到这些“互联网公司”的启迪，老牌的软件厂商，也“快速迭代”了起来。2017年11月，苹果的macOS爆出登入验证漏洞。记得我们上文提到的“根用户”权限吗？入侵者连用多个漏洞才这个权限。macOS刚发10.13.0的时候，任何用户轻轻松松就可以得到：用户名填“root”，密码栏留空，多按几次“解锁”按钮，就可以获取根用户权限了。就这么简单。

这还没完。漏洞公布18个小时之后，苹果就推出紧急补丁修复问题，效率很高。可是，苹果自己的macOS 10.13.1更新包却与补丁有冲突，如果用户先打补丁再升级10.13.1，补丁会被覆盖，漏洞又回来了。

macOS 10.13还有更过分的错误：在加载加密过的APFS硬盘的时候，系统会问你要密码（因为硬盘是加密的），此时，密码提示栏本来应该显示“密码提示”的（比如“你的生日+宠物的名字”之类的），当时密码提示栏会直接显示你的密码，应该说真的是非常有效的提示。

当然，也不是只有苹果如此随性。苹果的老冤家微软，也搭上了“敏捷开发”的快车。微软说，Windows 10不止是操作系统了，而且是一个“服务”，所以不是几年更新一次，而是一年更新几次。经常更新当然不是坏事，不过微软的更新方法强硬，所以出现了各种更新“事故”：比如游戏主播正在直播，Windows突然强制更新然后重启；或者用Window跑数据运算，第二天回来一看发现被强制更新了，运算结果没了。

去年10月的时候，微软还被迫停发一个更新版本，因为更新之后用户文件丢了。

Windows更新这么麻烦，于是很多人干脆就把更新关掉了，安全度还不如以前几年更新一次的时候。

## 要放弃隐私保护吗

> 应该承认，在现在这个时代，并不存在既方便又有效的隐私保护方法。

操作系统安全事故频发，开源软件也时不时爆出重大漏洞，那如果我们在乎自己的隐私，不想被人监控，那应该怎么办？

最直接的办法，是少用电子设备。我认识两个人，就是完全不用智能机的，没有微信、WhatsApp之类的通讯工具，要找他们就发邮件、打电话。这个方案相对安全，可是我相信大多数人是做不到的。

也有的朋友说，只要不用“国产机”就可以了，手机用iPhone，电脑不买联想，那就可以了。从NSO的案情来看，这个方案不成立，因为NSO入侵并不依赖政府提前埋下的后门。

熟悉技术的朋友，可能会学习各种隐私保护技巧：不要点陌生人的链接，给电子邮件加数字签名，浏览器禁用JavaScript，密码不能重复使用，等等；然后再加上各式软硬件：全硬盘加密，硬件密钥，笔记本摄像头盖……

“技术流”的问题是，很难坚持。各种隐私保护的手段其实无穷无尽，聊天工具加密了，是不是要再挑个安全小众的操作系统？操作系统换了，干脆手机也换一个开源的吧？手机换了，电脑要不要换？这一套都做下来，也不用工作生活了。

我觉得，应该承认，在现在这个时代，并不存在既方便又有效的隐私保护方法。可能值得一试的，是分层隐私：在平常生活中，不太重要的信息，放弃保护。网上购物，会让平台

知晓自己购买的东西，那就让它知道吧。要跟内地的朋友聊天，微信没有端到端加密，后台肯定全部记录了，那就让他们记录吧。

但在重要、值得保护的信息上，穷兵黩武。网上买一些不方便让人知晓的东西，那就用一次性电话注册一个新号，支付用一次性借记卡。如果是从事新闻、法律等敏感工作，那一台工作电脑，与日常使用分离，在电脑上装置防火墙，设白名单、长密码，甚至加载USB自毁程序，一旦不认识的USB设备插入，就销毁硬盘数据。

如此分隔“低隐私”与“高隐私”范围，或许能够在隐私保护和正常生活之间，有个平衡。

**（乐之，前端传媒数据记者）**

互联网　　网络安全


如果你喜歡
就分享給更多人吧

## 热门头条

1. 2019区选开票中：泛民主派已得逾380席，建制派溃败，多个主要人物连任失败
2. 理大冲突：被围两日，逾百名学生被带领离场，校园仍有示威者未撤走
3. 谁发明了新疆再教育营？《纽约时报》获400页文件揭其政治动员过程
4. 【数据透视】稳胜或险胜？建制民主阵营区选数据这样说
5. 专访陈方安生：我们与中央似乎没有一个好好的沟通渠道
6. 读者来函：作为内地生，留守中大是怎样的体验？
7. 那些负债累累的地方政府：钱是怎么借的、又该如何还？
8. 金马、金鸡隔岸赛果：平行时空各自安好，华语电影的未来将要如此吗？
9. 中大事件后返台学生：“每天出门前，习惯先看台北捷运有没有停驶”
10. 内地眼中的香港局势：被刻意制造的“仇恨”舆论

## 编辑推荐

1. 缅甸有媳妇（下）：河南相亲团的缅北“爱情”之旅
2. 缅甸有媳妇（上）：缅甸姑娘的“孤身”中国婚礼
3. 季文仪：从罗永浩那里，我们还能期待什么？
4. 逾越与隔限：反修例运动中的女性力量及性别策略
5. 王宏恩：台湾不分区立委名单，民进党、小党、郭柯的选择
6. 钟剑华：逆转的香港区选后，各方的政治责任
7. 那些负债累累的地方政府：钱是怎么借的、又该如何还？
8. 这一切得来不易：金马五十六的历史价值

9. 金马、金鸡隔岸赛果：平行时空各自安好，华语电影的未来将要如此吗？

10. 【数据透视】稳胜或险胜？建制民主阵营区选数据这样说

## 延伸阅读

### “翻墙”攻防战：举国围剿下，VPN 真的可以被干掉吗？

围绕防火长城展开的“砌墙”、“拆墙”技术多年来一直不断博弈，但当技术解决不了燃眉之急时，简单粗暴的行政手段才是最终的“大杀器”。

### 陈至洁：鸟笼中的微信，与“插翅难飞”的中国境外网民

中国政府严加控管并强力引导互联网的公共信息内容，甚至产生了境外的问题。中国政府对微信用户的文化思想控制，并不会因为人移居海外而减少，因为只有中国的公民或在中国登记的公司才能营运微信公众号并提供其信息内容……

### 洛德：在“被豢养”的互联网世界，批评百度时我们忽略了什么？

认清自己正在被豢养的事实，以及周遭世界的危险，这在互联网时代是有益无弊的。

### 读者来函：当港人用科技工具动员百万人上街时，我们如何用它保护自己？

一个混迹互联网20年的网民写下的网络安全“懒人包”。