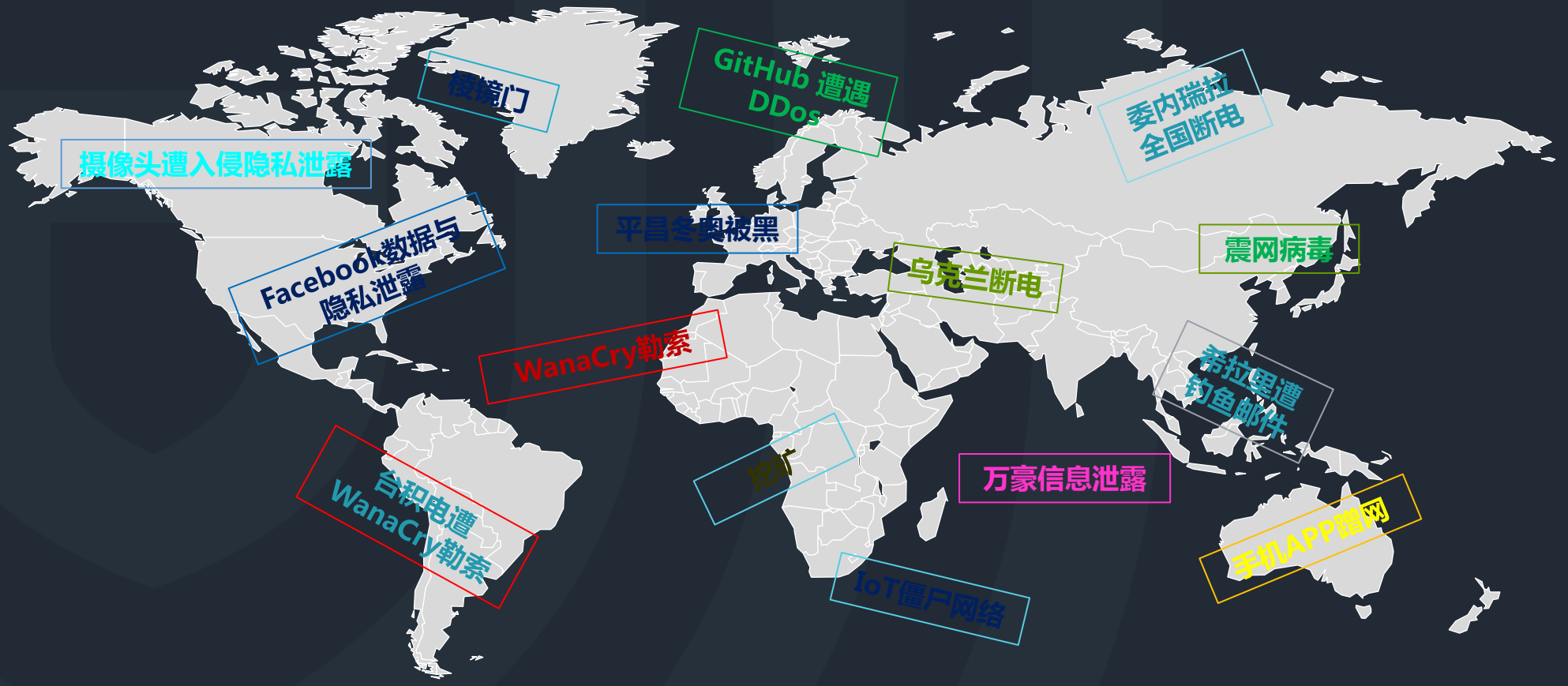
安全方法论之
“军火化”网络攻击形式及防护方法论

01 网络安全的“故事”

网络安全事件关键词



“四个假设”正在逐渐变为确定现实——

- 假设系统一定有未被发现的漏洞
- 假设一定有已发现但仍未修补的漏洞
- 假设系统已经被渗透
- 假设内部人员不可靠

网络安全事件频发的原因

1

数字化转型引发的三大安全威胁

网络犯罪

个人信息滥用，数据泄露、网络诈骗，数据窃取

关键信息基础设施攻击

勒索攻击、敏感数据窃取，直接威胁国家稳定和经济运行

国家对抗和网络空间利益重新划分

商业利益诉求和恐怖破坏目的交织，高智商利用高技术集团化对抗升级

2

“四个假设”正在逐渐变为确定现实

- 假设系统一定有未被发现的漏洞
- 假设一定有已发现但仍未修补的漏洞
- 假设系统已经被渗透
- 假设内部人员不可靠

3

引发网络犯罪的五个动机

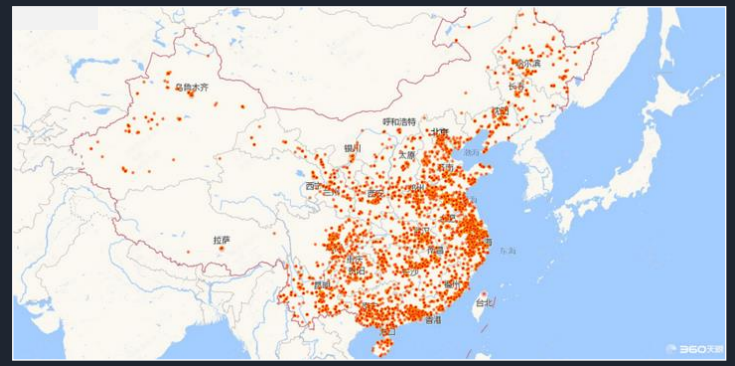
归纳出七类有代表性的网络安全事件

- 勒索
- 信息泄露
- DDoS攻击
- 可利用漏洞被曝光
- 破坏国家关键基础设施
- 新技术引发的新型攻击
- 其他

No1. 勒索：WannaCry 索要比特币

事件概况

2017年5月12日，黑客组织利用泄露的NSA黑客数字武器库中“永恒之蓝”工具发起蠕虫病毒攻击进行勒索，中毒计算机文件将被锁定，需支付赎金比特币才能解锁。



影响范围

- 勒索软件已攻击99个国家的数千家企业及公共组织，美国至少1600家、俄罗斯至少11200家受到攻击
- 我国感染范围覆盖了几乎所有地区，遍布高校、加油站、医院、政府办事终端等各大领域，超30万台机器中招，至少有28388个机构被感染

事件分析

- 虽然下黑手者目前还找不到，但其所用的工具，却明确无误地指向了一个机构——NSA，永恒之蓝就是NSA针对微软MS17-010漏洞所开发的网络武器，2013年6月，“永恒之蓝”等十几个武器被黑客组织“影子经纪人”（Shadow Brokers）窃取并公布；
- 2017年3月，微软已经放出针对这一漏洞的补丁，但是一方面由于一些用户没有及时打补丁的习惯，二是全球仍然有许多用户在使用已经停止更新服务的Windows XP等较低版本，无法获取补丁，因此在全球造成大范围传播。

启示：打补丁这件事不要心存侥幸！

No1. 勒索：新一轮勒索“Petya”演变为无法修复的破坏

事件概况

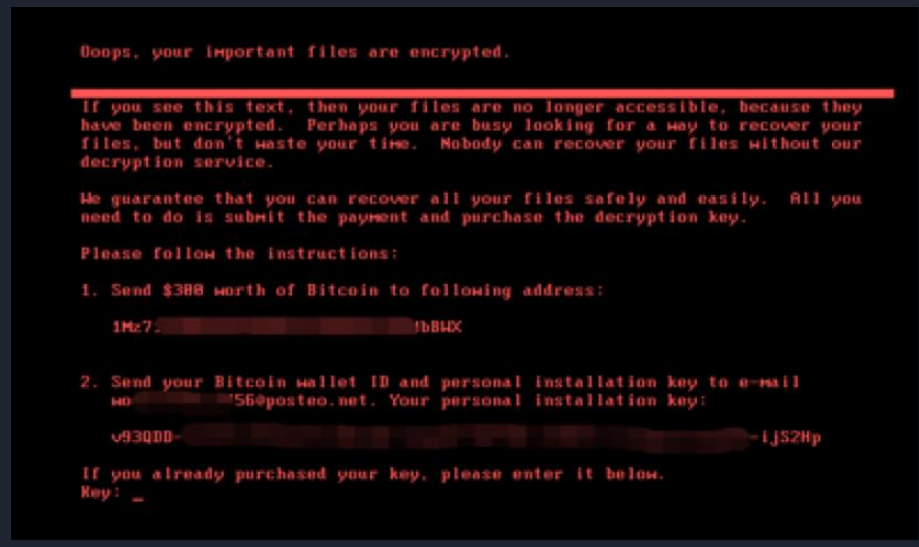
“WannaCry”还没有结束，2017年6月27日，新一轮勒索病毒“Petya”袭击了欧洲多个国家，包括乌克兰、俄罗斯、印度、西班牙、法国、英国、丹麦等国在内都遭受了攻击;

事件影响

此病毒相比“WannaCry”更具破坏性,开机界面上留下来的信息即使提供给黑客也是没有办法进行解密的，因此，不得不怀疑此次“Petya”病毒的真正目的。“Petya”更像是在做有目的性的攻击，对目标进行无法修复的破坏性攻击，而并非以敲诈勒索为目的。

事件分析

Petya同样利用了MS17-010(永恒之蓝)的SMB漏洞，感染局域网中开放445端口的所有终端及服务器。



启示：

（1）同样的漏洞有可能被重复利用；

（2）新一轮勒索软件的重要新用途之一不仅是敲诈勒索，而是无法修复的破坏！

No1. 勒索：GlobeImposter（江湖骗子）有价值目标的定向攻击

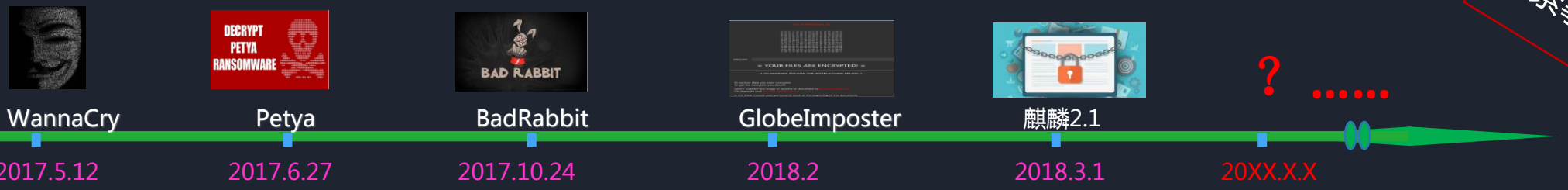
事件概况

2018年2月某日上午8时左右，儿童医院核心业务系统无法正常使用，经查系服务器中了最新勒索病毒：“业务系统设备处于关闭状态，业务服务器数据文件被加密”，事件影响恶劣，给医疗就诊的秩序、患者生命安全构成了极大威胁。

入侵方式

此次感染的勒索软件为GlobeImposter，通过RDP远程桌面入侵施放病毒，加密本地磁盘与共享文件夹的所有文件。GlobeImposter勒索病毒有变种，在国内医疗行业爆发较为集中。

勒索事件的启示一：勒索事件曾经发生过、当下正在发生、未来也不会停止！



勒索事件的总结与分析

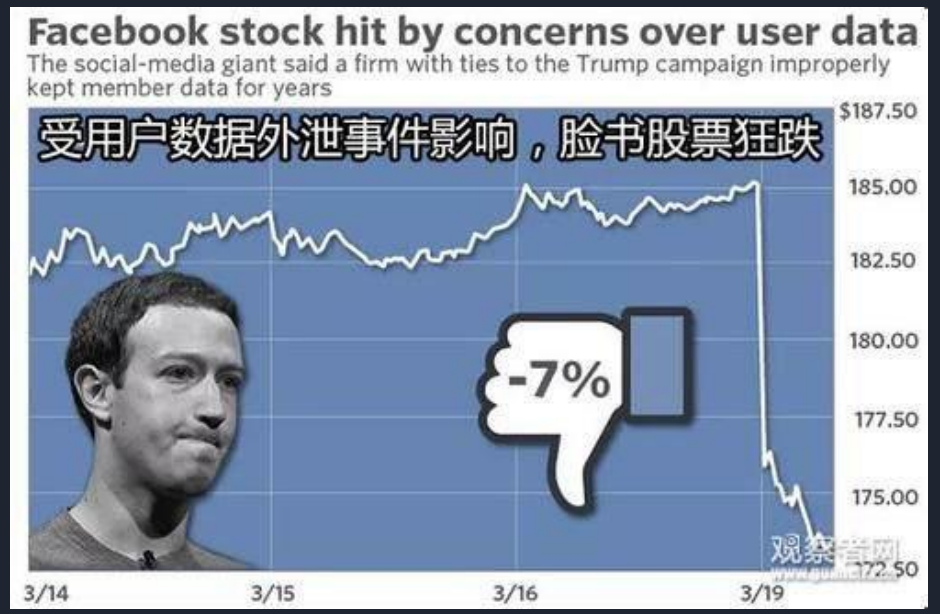
勒索事件的启示二：勒索病毒的发展趋势

1. 利用漏洞和弱口令植入勒索的案例增多
2. 勒索病毒持续更新迭代对抗查杀
3. 针对有价值目标发起定向攻击逐渐增多
4. 从单一勒索向勒索与无法修复的破坏发展

No.2 信息泄露：Facebook泄露大量客户隐私

Facebook用户数据泄露

- 2018年Facebook上超过5000万用户信息数据被一家名为“剑桥分析(Cambridge Analytica)”的公司泄露，用于在2016年美国总统大选中针对目标受众推送广告，从而影响大选结果。此时，公众才恍然大悟，在特朗普成功当选的背后有着这家剑桥分析公司的数据支撑。
- 该事件不是通过黑客攻击手段获取的数据，而是由于对第三方的协议漏洞以及监管失效造成的。



除了股票下跌，Facebook还将面临GDPR开出的巨额罚单！

2000万欧元或者是上个会计年度里全球年收入的4%

No.2 信息泄露：希拉里竞选团队被邮件钓鱼致信息外泄

2013年前	•希拉里任国务卿期间，不按规定使用政府邮件，事发接受调查前删除3万封邮件
2016年3月	•希拉里竞选团队主席（John Podesta）邮箱遭钓鱼攻击，邮箱密码被盗导致邮件泄露
10月9日	•维基解密公布了数千封John Podesta被黑的邮件
10月25日	•黑客Kim Dotcom公开3万封被希拉里删除的邮件内容

- 2016年3月19日，希拉里竞选团队主席约翰·波德斯塔（John Podesta）收到了一封貌似来自Google的警告邮件，然而，该邮件却是一封窃取个人信息的钓鱼邮件，幕后攻击者被认为是俄罗斯国家黑客。
- Podesta无意点击了邮件中的恶意链接，其邮箱密码就成了黑客的“囊中之物”，由此造成其与希拉里往来的重要邮件泄露。
- 希拉里竞选期间，被“钓鱼邮件”攻击后泄露的邮件内容被频繁爆出。

No.2 信息泄露：万豪酒店被APT入侵拖库

万豪旗下喜达屋酒店5亿条信息泄露

- 2018年11月，万豪国际集团在官方微博账号上表示，其公司旗下喜达屋酒店的一个客房预订数据库被黑客入侵，多达5亿人次的详细信息可能遭到泄露。泄露数据库中包含约5亿名客人信息，其中高达3.27亿人次的泄露信息包括名字、邮寄地址、电话号码、护照号码、生日、到达和离店信息等。
- 自2014年起，即存在第三方对其旗下喜达屋网络未经授权的访问。黑客入侵后不破坏数据，只潜伏，在服务器里安置“后门”，达到源源不断获取最新数据的目的。而对于最初黑客是如何“入侵”喜达屋系统的，目前没有明确公布，但针对企业数据库的攻击手段很多，简单的如弱口令暴力破解、SQL注入等。

外部威胁

- 弱口令暴力破解
- WEB漏洞，如SQL注入、XSS
- 钓鱼邮件等APT入侵

内部管理

- 开发人员违规外传
- 生产及测试数据混用
- 内部人员误操作
- 内部人员特权或越权主动获取并泄密

第三方

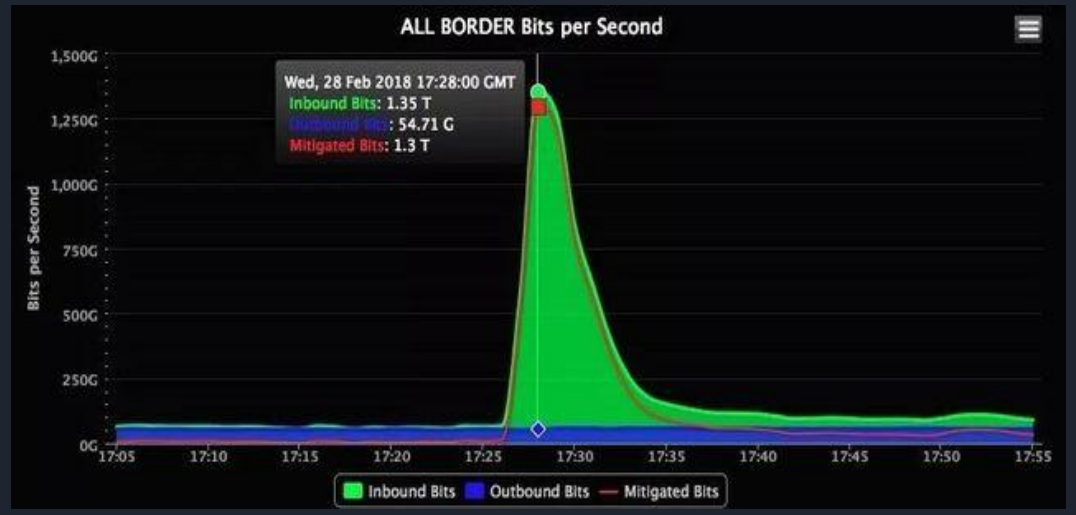
- 外包商泄密
- 与第三方数据传输过程泄密

信息泄露事件途径分析

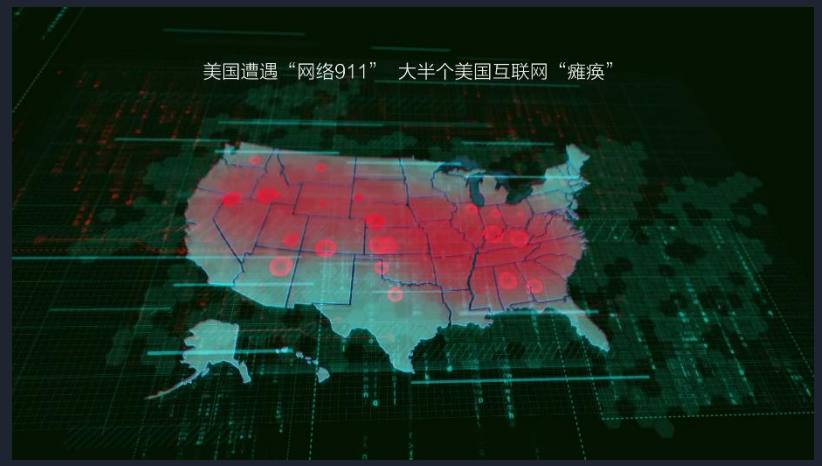
No.3 DDoS攻击

Github遭遇史上最大1.35 Tbps DDoS攻击

- 2018年美国东部时间下午 12:15，知名代码托管网站 GitHub 遭遇了史上最大规模的 DDoS 网络攻击，每秒 1.35 TB 的流量瞬间冲击了这一开发者平台。
- 本次攻击并非依赖于传统的僵尸网络，而是使用了 Memcached 服务器。该服务器的设计初衷是提升内部网络的访问速度，而且是不应该被暴露在互联网中的，但是至少有超过 5 万台此类服务器连接到了服务器上，因此非常容易受到攻击。犯罪分子可利用 Memcache 服务器通过非常少的计算资源发动超大规模的 DDoS 攻击，该漏洞是由于 Memcache 开发人员对 UDP 协议支持方式不安全所导致的。



No.3 将移动APP、智能设备沦为僵尸的DDoS攻击



mirai僵尸网络发动的DDOS攻击-美国断网

- 2016年10月21 日晚间，美国大面积断网事件。Twitter、亚马逊、华尔街日报等数百个重要网站无法访问，美国主要公共服务、社交平台、民众网络服务瘫痪。
- 事件原因是攻击者对美国互联网域名解析服务商DYN进行了DDoS攻击，mirai僵尸网络操控的全球约89万台智能设备，就是攻击流量的主要来源.在这次灾难中，仅DYN公司的直接损失就超过了1.1亿美元。

将移动设备沦为肉鸡的应用层CC DDoS攻击

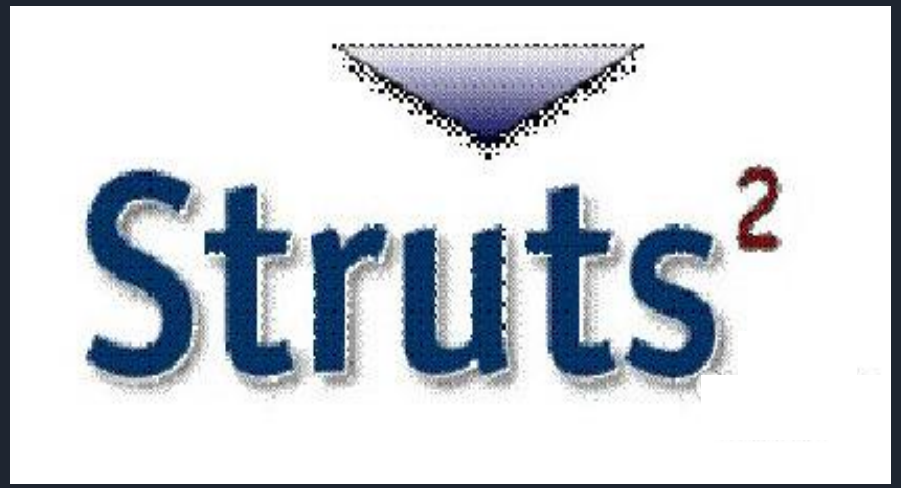
近期，阿里云安全团队观察到数十起大规模的应用层资源耗尽式DDoS攻击（应用层CC攻击）。溯源发现，这些攻击事件源于大量用户在手机上（同时支持安卓及iOS）安装了某些伪装成正常应用的恶意APP，该APP在动态接收到攻击指令后便对目标网站发起攻击。根据阿里云安全团队监测的数据显示，近两个月，已经有五十余万台移动设备被用来当做黑客的攻击工具，达到PC肉鸡单次攻击源规模。

僵尸的感染对象已经从服务器、PC，扩展向智能手机APP、摄像头、路由器、家居安防系统、智能电视、智能穿戴设备，甚至是婴儿监视器。

No.4 可利用的漏洞被曝光

Apache Struts 2被曝存在远程命令执行漏洞

2017年3月，Apache Struts 2被曝存在远程命令执行漏洞， Struts2漏洞涉及Struts2.0及以上的版本是一个远程命令执行漏洞和开放重定向漏洞。利用漏洞,黑客可发起远程攻击,不但可以窃取网站数据信息,甚至还可取得网站服务器控制权。而且,目前针对此漏洞的自动化工具开始出现,攻击者无需具备与漏洞相关的专业知识即可侵入服务器,直接执行命令操作,盗取数据甚至进行毁灭性操作。



英特尔处理器“Meltdown”和“Spectre漏洞”

2018年1月，英特尔处理器中被曝出存在“Meltdown”（熔断）和“Spectre”（幽灵）两大新型漏洞，包括AMD、ARM、英特尔系统和处理器在内。影响范围波及近20年所发售的手机、电脑服务器及云计算产品。这些漏洞的存在允许恶意程序从其他程序的内存空间中获取信息，换句话说，内存的信息都可能外泄，例如账户信息及密码等等。

No.4 可利用的漏洞被曝光

影子经纪人公开NSA黑客武器库

2017年4月14日，影子经纪人（Shadow Brokers）在steemit.com上公开了一大批NSA（美国国家安全局）“方程式组织” (Equation Group)使用的极具破坏力的黑客工具，其中包括可以远程攻破全球约70%Windows机器的漏洞利用工具。

任何人都可以使用NSA的黑客武器攻击别人电脑。其中，有十款工具最容易影响Windows个人用户，包括永恒之蓝、永恒王者、永恒浪漫、永恒协作、翡翠纤维、古怪地鼠、爱斯基摩卷、文雅学者、日食之翼和尊重审查。黑客无需任何操作，只要联网就可以入侵电脑，就像冲击波、震荡波等著名蠕虫一样可以瞬间血洗互联网。该组织还未将泄露的美国安全局的黑客工具全部公开，一旦公开，后果可能会危及数十亿的软件用户。

WannaCry的攻击依赖于影子经纪人窃取并释放的网络武器，下一个目标会是谁呢？

No.5 破坏国家关键基础设施

乌克兰电网系统遭受攻击

- **事件概况**

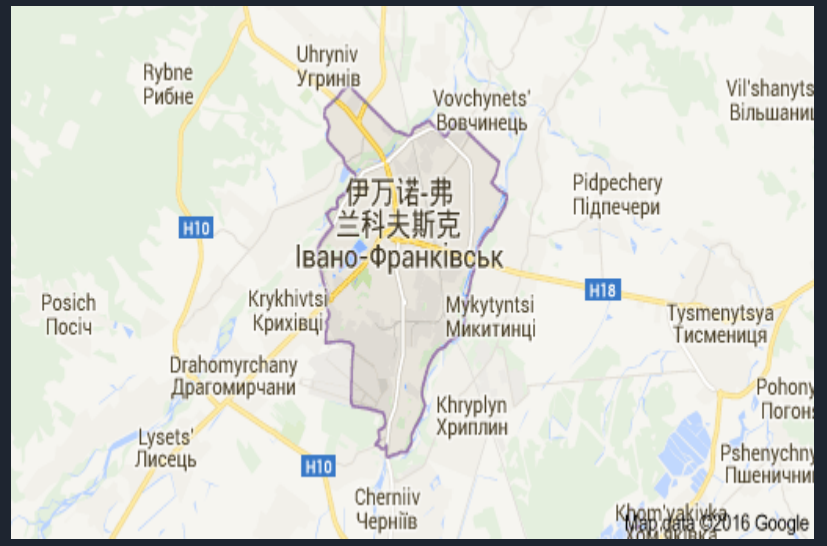
  2015年12月23日下午，乌克兰电网系统遭受到SandWorm（沙虫组织）恶意代码攻击，导致乌克兰首都基辅部分地区和乌克兰西部伊万诺-弗兰科夫斯克地区（乌克兰超过一半的地区）断电几个小时，约140万名居民受到影响。

- **事件起因**

  黑客利用欺骗手段让电力公司员工下载恶意软件“BlackEnergy”，利用此软件将电力公司主控电脑与变电站断开连接，在系统中植入病毒让电脑全体瘫痪，同时切断居民与电力公司的电话通讯。

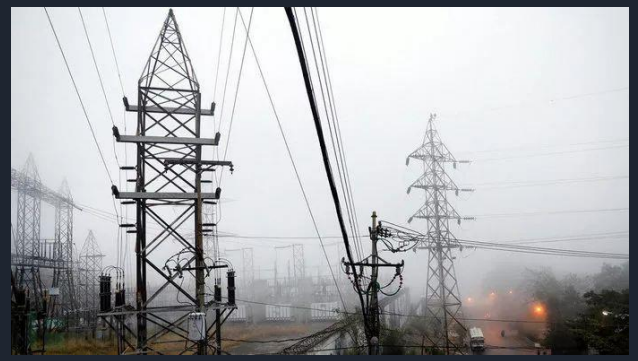
- **事件结论**

  ESET 公司表示，此次乌克兰大规模的停电主要是电力系统的设计出现漏洞，使得黑客轻易入侵 Microsoft Office 文档。ICS-CERT警告称BlackEnergy主要会对下面的三种HMI产品展开攻击：GE Cimplicity、 Advantech/Broadwin WebAccess和西门子WinCC。



No.5 破坏国家关键基础设施

委内瑞拉全国性断电事件

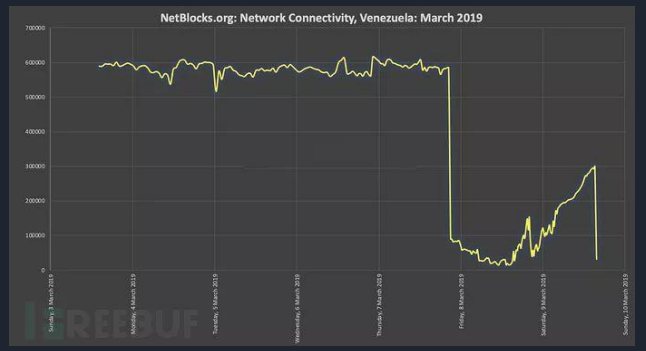


事件概况

- 2019年3月7日晚，委内瑞拉在3月7日下午和晚间遭遇了波及全国的大范围停电，是该国史上规模最大的停电事件之一，23个州中仅有5个未受波及。
- 9日上午，全国70%的地方恢复了供电，但没过多久电子系统再次遭到”高科技手段”实施的电磁攻击，导致再次大范围的停电。
- 大规模停电后，委政府指责外部和极右势力在国内制造“电力战争”。

网络攻击手段

- 其一，利用电力系统的漏洞植入恶意软件
- 其二，发动网络攻击干扰控制系统引起停电
- 其三，干扰事故后的维修工作



事件分析

这次电力系统遭受攻击的目的，就是要瘫痪委内瑞拉民生基础，彻底瓦解民心，从而“手不血刃”，达到目的，支持反对派上台。

No.5 破坏国家关键基础设施

加密货币挖矿软件导致欧洲废水处理设备瘫痪

2018年2月，工业网络安全企业 Radiflow 公司发现四台接入欧洲废水处理设施运营技术网络的服务商遭到了加密货币挖矿软件的恶意入侵。由于受感染的服务器人机交互（简称HMI）设备被加密货币挖矿软件拖垮了CPU，致使欧洲废水处理服务器瘫痪。

工业环境网络中，负责运行敏感 HMI 与 SCADA 应用程序的 PC 设备无法获得最新的 Windows 、反病毒以及其它重要更新，因此将始终面临严重的潜在恶意软件攻击。

共享别人的资源

挖掘自己的财富

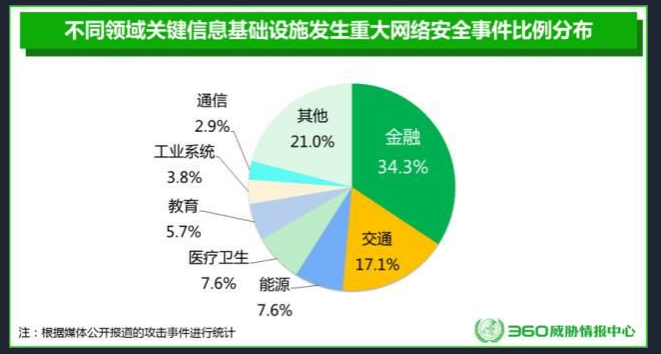
攻击特点

窃取网络资源，挖掘数字货币

自动扫描攻击，漏洞无法幸免

一场国家间“0和1”的战争

作为现代战争的一个重要作战手段，通过网络攻击打击对手的国家基础设施，从而造成生产停止、通信中断、交通瘫痪、能源供给不足等重大损失，其破坏性远胜于常规炮火的打击，甚至可以决定战争的走势。

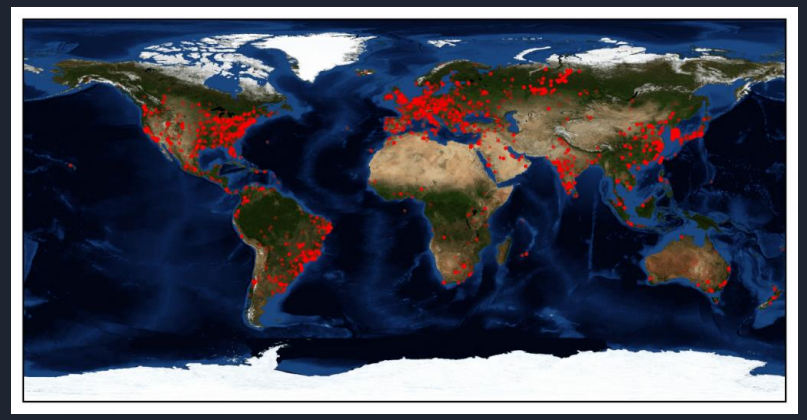


金融、交通、能源等领域
最容易遭受网络攻击

No.6 新技术发展带来的隐患—物联网（摄像头）

摄像头沦为僵尸网络

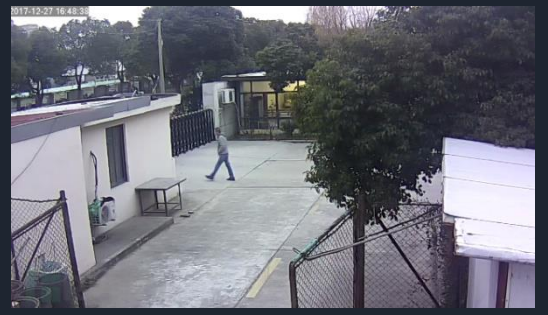
- 安全研究人员发现一种新型IoT僵尸网络，代号卫Hide'N Seek (HNS“捉迷藏”）。主要针对的是不安全IP摄像头。HNS僵尸网络对具有开放Telnet端口的设备发起暴力破解攻击，具有高度的自定义特征。
- 上线不满一个月HNS僵尸网络肉鸡数量从12台猛增至3.2万台；5月末，感染超过9万台设备。
- 同时，研究者发现HNS增添了新功能，在设备重启之后，恶意软件依旧存在。HNS成为首个能在设备重启后存活下来的同类恶意软件，开启了僵尸网络的“新时代“。

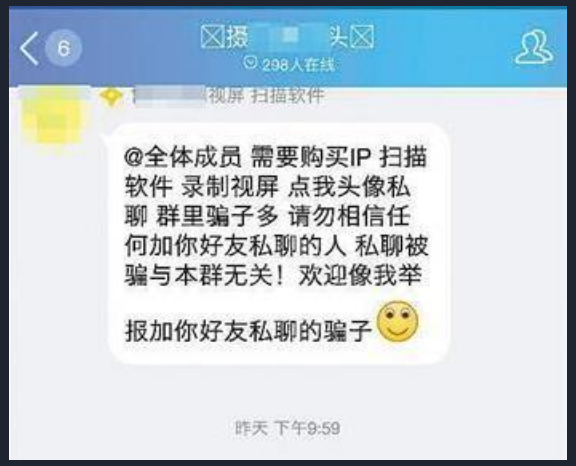


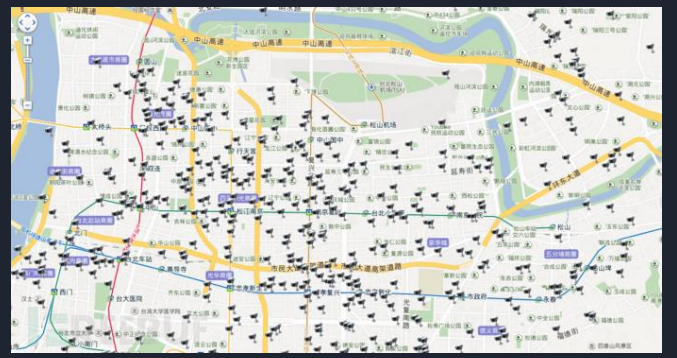
随时可以发起DDoS攻击

通过摄像头暴露的生活隐私

黑色产业可以通过暴露的物联网设备采用多种方式潜入你的生活，并把你的生活录制下来为其获利。更多情况下，使用网络的公开技术资源就能够查到网络空间中存在安全威胁的物联网设备，从而使你的生活变成一场「直播秀」





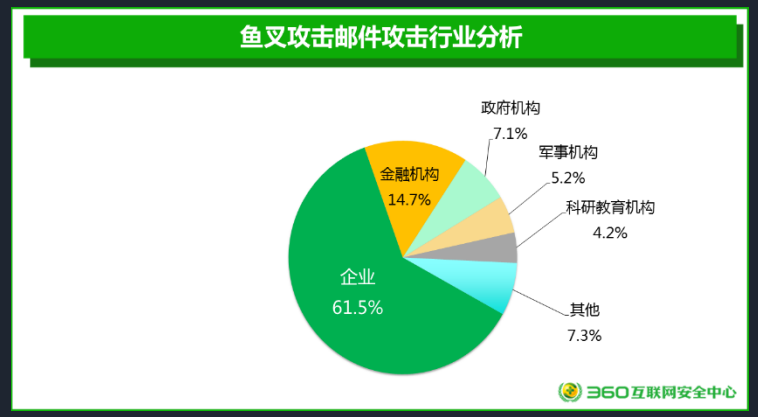


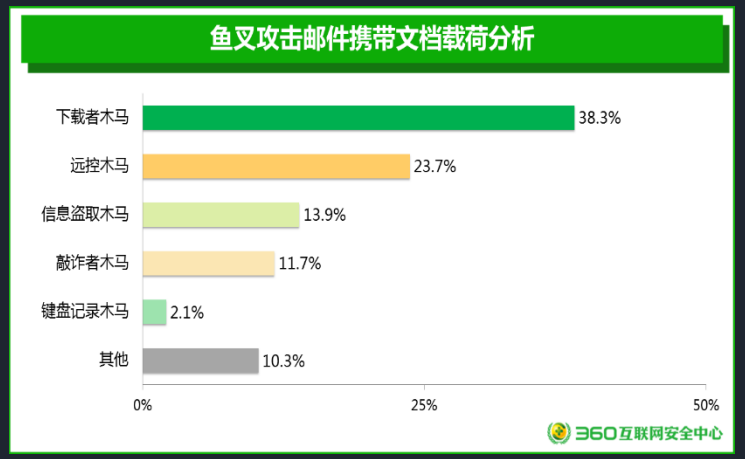
使用网络空间搜索设备SHODAN，以webcam、camera2个关键词为例，仅在中国地区就有81,084个属于存在安全隐患设备的公网IP地址暴露。左图为台北市区摄像头暴露密集程度。

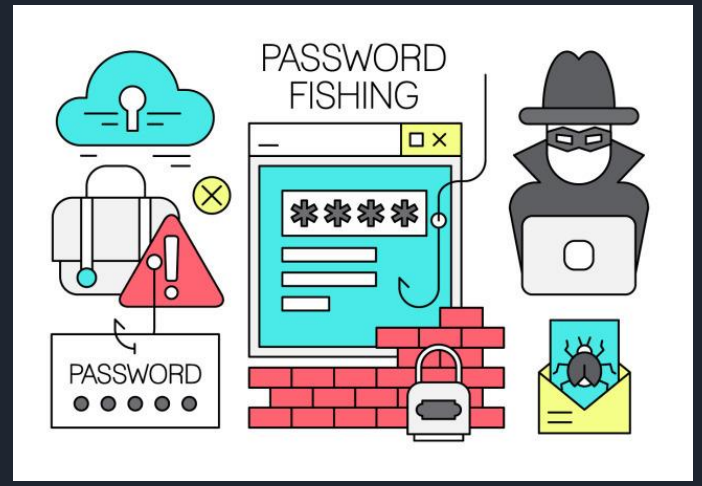
No.7 其他——钓鱼邮件

2018年2月，韩国平昌冬奥会开幕式期间，主办方遭遇身分不明的黑客攻击，服务器被入侵。因担心黑客采取下一步行动，主办方关闭服务器，官网宕机12小时，观赛门票无法打印导致观众无法正常入场，媒体中心系统故障导致观众无法观看直播……

McAfee报告称，早在赛事举办前，众多为赛事提供基础设施服务的相关机构遭受了精心伪装、植入恶意软件的鱼叉式钓鱼邮件攻击，黑客目的旨在窃取敏感信息或财务数据。







鱼叉式钓鱼邮件攻击是APT的惯用手法，其精要在于通过面打击，突破防御对象最薄弱的成员。防御时，应对可疑邮件一个都不放过，通过对邮件细微之处的鉴别，对邮件是否具有威胁进行告警。

No.7 其他——内部人员作案

Facebook

特权账号

- 2018年5月初，Facebook公司解雇了一位安全工程师，因为其曾利用访问个人数据的特权在线跟踪并骚扰女性。此外，该安全工程师还在约会平台Tinder上向好友吹嘘自己可以看到任一 Facebook用户的个人资料。
- 据悉，在 Facebook 公司内部有个小组，有权限观看任何用户的个人资料，当然，这名安全工程师的案例并不是孤立的，还有多名Facebook员工同样因为滥用用户私人信息而遭到解雇。由于此事曝光的时间点距离“泄露门”事件发生不久，可以说是进一步打击了Facebook的用户信任。

特斯拉（Tesla）

内部人员

2018年6月，特拉斯指控了一名前员工Martin Tripp，称其编写了侵入特斯拉制造操作系统的软件，并将几个GB的特斯拉数据传输给外部实体。这些数据包括数十张机密照片和特斯拉制造系统的相关视频。除此之外，特斯拉还声称Tripp编写了计算机代码，定期将特斯拉的数据输出给公司以外的人。

Nuance

离职人员

美国医疗语音识别软件开发商Nuance的一名前员工，在离职后登陆公司服务器，访问并泄漏了4.5万名客户的信息，包括生日、医保账号、健康状况、治疗情况等。

启示：万物皆变，人是安全的尺度

No.7 其他——不安全的APP

WiFi蹭网被曝光

2018年4月，工信部对WiFi万能钥匙等号称“免费上网”类App展开调查。据悉，此类“蹭网”App主要是免费向用户提供使用他人WiFi网络的功能，涉嫌窃取个人信息及入侵他人WiFi网络。工业和信息化部网络安全管理局调查发现这类App具有共享用户所登录WiFi网络密码等信息的功能。

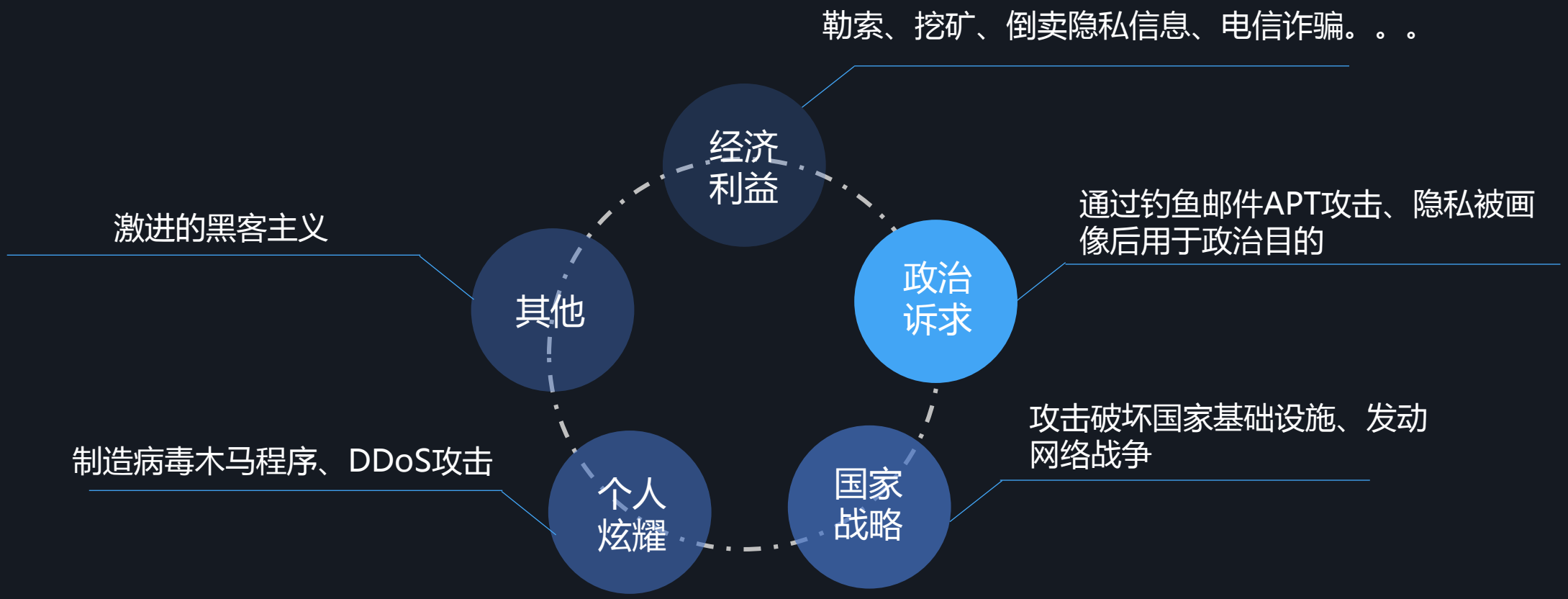
APP过度收集用户隐私

- QQ音乐等18款APP疑似存在过度收集短信、通讯录、位置、录音等用户敏感信息；
- 万能看等9款APP疑似存在未经用户同意收集使用用户个人信息。

“寄生推”恶意病毒

2018年4月，腾讯安全反诈骗实验室发现一款针对安卓手机的恶意病毒——“寄生推”。该病毒涉及300多款App，受影响用户高达2千万人。据了解，“寄生推”可通过预留的“后门”云控开启恶意功能，进行恶意广告弹出和强制应用推广。

事件背后的原因分析


勒索、挖矿、倒卖隐私信息、电信诈骗。。。
经济利益
通过钓鱼邮件APT攻击、隐私被画像后用于政治目的
政治诉求
攻击破坏国家基础设施、发动网络战争
国家战略
制造病毒木马程序、DDoS攻击
个人炫耀
激进的黑客主义
其他

02 网络安全的新形势

网络安全新常态

1、漏洞军火化，军火民用化

“永恒之蓝”勒索事件

- 网络军火民用化的代表性事件：攻击者所用的攻击方法与被泄露美国NSA网络武器“永恒之蓝”有关
- 一个重要漏洞的价值不亚于一枚导弹，漏洞已经变成了稀土、原油一样的国家战略资源。

网络安全新常态

2、网络攻击产业化，网络犯罪集团化

- 恶意网络攻击出现成熟黑色产业链：

DDoS攻击已形成了包括木马作者、网络黑客、地下承包商、网络黑帮和客户五种角色的产业链。

- 网络诈骗从业人口160万+：

形成一条完整、分工明确的地下黑产链，可划分多达15个工种，非法“年产值”超过1152亿元。

网络安全新常态

3、应急响应争分夺秒

- 今年6月，中央网信办印发的《国家网络安全事件应急预案》规定， 属特别重大网络安全事件的，要及时启动I级响应，成立指挥部，应急办24小时值班。
- 72小时抗击勒索蠕虫病毒：5月处理“永恒之蓝”事件时，奇安信在第一时间与主管部门取得联系，随时通报进展，反应效率用时间衡量，是小时级的。

网络安全新常态

4、“重保”常态化

北京、辽宁、
四川、河南、
湖南、浙江、
广东、福建等多地

重大网络安全保卫活动

2016.9 G20峰会

2017.3 两会

2017.5 一带一路

2017.9 金砖会议

2017.9 国家网络安全周

2017.10 十九大

网络安全新常态

5、“等保”法制化

美国：2013年制定《提高关键基础设施的网络安全》，2014年 “关键基础设施网络安全框架规范”出台。

英国：2007年英国国家基础设施保护中心（CPNI）成立，为减少基础设施被恐怖主义破坏和其他威胁，保护通信、能源、金融、医疗、交通等基本服务安全。

德国：2015年通过《德国网络安全法》，明确“关键基础设施”运营者责任、扩大网络监管权、确定网络安全报告制度和增设电信运营商的义务 。

中国：2017年发布《网络安全法》，标志着我国网络安全管理进入法制时代，明确了法制下的各种权责及相关处罚。

03 网络安全的新方法论

四个假设

新一代网络安全体系思想

四个假设

系统一定有没被发现的漏洞

一定有已发现漏洞没打补丁

系统一定可以被渗透

内部人员一定会犯错

以“四个假设”为前提保障关基安全

四新战略

新战具：第三代网络安全技术

新战力：数据驱动安全

新战术：零信任架构

新战法：人+机器安全运营

以“四新战略”为原则设计关基安全方案

三位一体

高位能力

中位能力

低位能力

以“三位一体”方法搭建关基安全体系

三同步

同步规划

同步建设

同步运营

以“三同步”思想做好关基的体系化保障

三方制衡

用户

云服务商

安全公司

以“三方制衡”机制构建综合高效系统

遵循“四个假设”，建立全新的网络安全防护体系

第一个假设：系统一定有未被发现的漏洞

第二个假设：一定有已发现但仍未修补的漏洞

第三个假设：系统已经被渗透

第四个假设：内部人员不可靠

1 假设一：系统一定有未被发现的漏洞

2018年，国家信息安全漏洞共享平台CNVD共接收漏洞近10万个。

研究表明：程序员每写1000行代码，会出现一个漏洞

网络防护离不开软件和硬件，但软件和硬件的漏洞不可避免

2 假设二：一定有已发现但仍未修补的漏洞

5.12 “永恒之蓝” 勒索病毒事件

1. 3月份，微软发布了针对Win7及以上操作系统的安全漏洞补丁
2. 很多单位都没有及时安装更新，成了病毒“重灾区”
3. WinXP、2003等老旧操作系统，微软已不再提供安全更新，而国内大量机构仍旧在使用

3 假设三：系统已经被渗透

隔离网一度被认为是安全的

→ 恶意威胁的复杂性和多样性显著变化

→ 攻击入侵的路径不再局限于互联网攻击

2011年震网病毒事件

伊朗的核设施是一个物理隔离、高度防护的网络→攻击者用USB移动介质作为跳板，植入了木马文件，成功绕过安全产品的检测→利用Windows和西门子系统的漏洞，成功入侵了离心机的控制系统，干扰正常运行

3 假设三：系统已经被渗透

隔离网内的终端安全问题突出

1. 本地恶意代码防御能力比较弱
2. 病毒库更新频率不高

4 假设四：内部人员不可靠

2015年四川“扫雷”专项行动

1. 四名同一家国防军工单位的员工，分别被境外间谍情报机关发展利用；
2. 利用工作便利，向境外提供高新武器研发、测试、生产、列装部队等涉密情报信息;
3. 通过自身人脉关系，为境外间谍人员物色、推荐国防军工领域易被引诱利用的科研人员

1/4的数据泄露来自内部人员

外包服务商成为了新的安全威胁

4 假设四：内部人员不可靠

1. 无泄密动机：把核心资料存在云盘或U盘，没有将资料及时销毁/被钓鱼邮件、恶意软件利用

2. 有泄密动机：有意识有计划地破坏、盗取内部数据/主动利用内部管理漏洞或技术漏洞，进行踩点、试探、入侵、窃取等

85%的网络安全威胁来自于内部

04 | APT攻击简介

APT攻击是什么

- APT:高级持续威胁（Advanced Persistent Threat),普遍认可的定义是，利用各种先进的攻击手段，对高价值目标进行的有组织、长期持续性网络攻击行为。

特点：

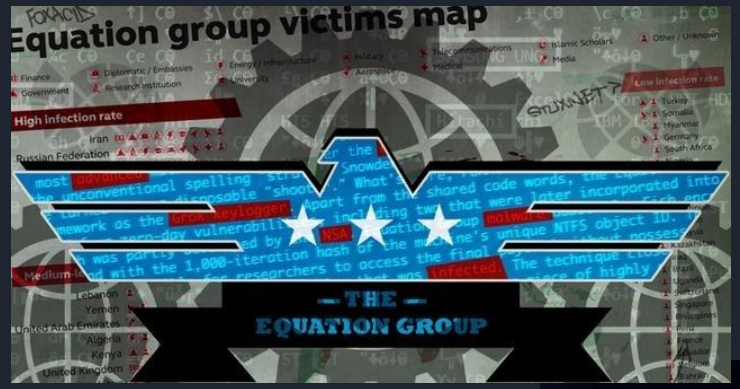
1. 高度目的性

2. 高度隐蔽性

3. 高度危害性

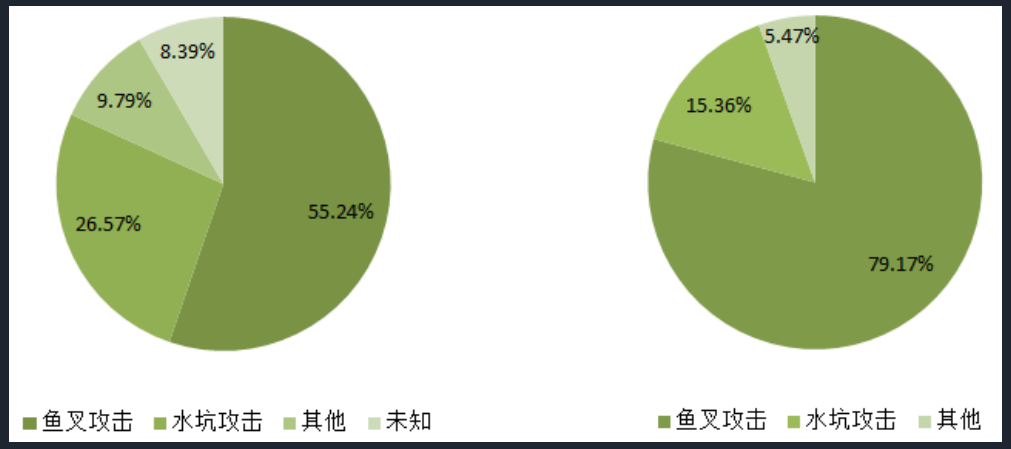
4. 目标实体化

5. 极强的持续性



APT攻击介绍-鱼叉

- “鱼叉攻击”是黑客攻击方式之一，最常见的做法是，将木马程序作为电子邮件的附件，并起上一个极具诱惑力的名称，发送给目标电脑，诱使受害者打开附件，从而感染木马。



APT攻击介绍-鱼叉

- 邮件的标题、正文和附件都可能携带恶意代码，目前主要的方式是附件是漏洞文档、附件是二进制可执行程序和正文中包含指向恶意网站的超链接这三种，进一步前两种更为主流

相关伪装项	具体内容
文件名	1、 与邮件内容、诱饵文档内容相符的文件名； 2、 超长文件名，其目的是隐藏文件扩展名。
文件扩展名	1、 双扩展名，采用 RLO[4]伪装扩展名。伪装的文档扩展名以“.doc”等微软 office 系列为主，另外伪装的图片扩展名以“.jpg”等为主； 2、 双扩展名，不采用 RLO 方式。
文件图标	1、 文档图标，以微软 office 系列中的 word、excel 文档图标为主； 2、 文件夹图标； 3、 图片图标。

APT攻击介绍-鱼叉

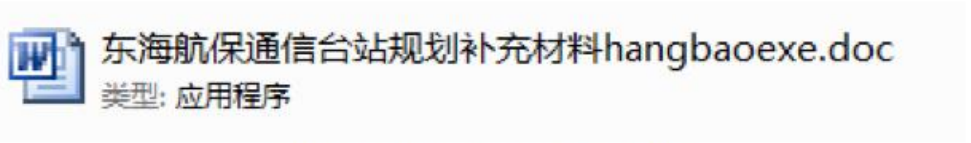


图 7 RLO 伪装扩展名（白海豚组织）

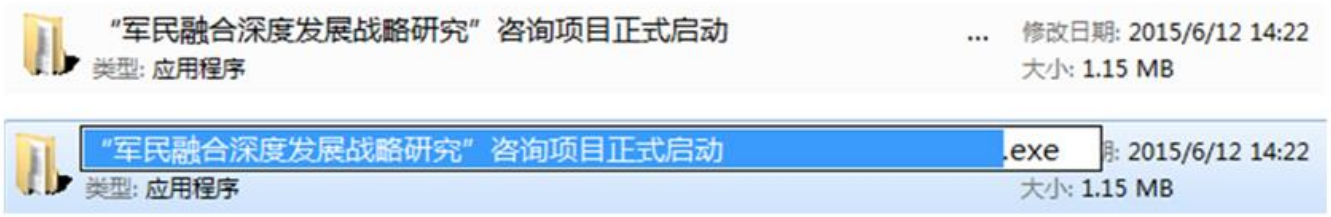


图 8 超长文件名和文件夹图标（白海豚组织）

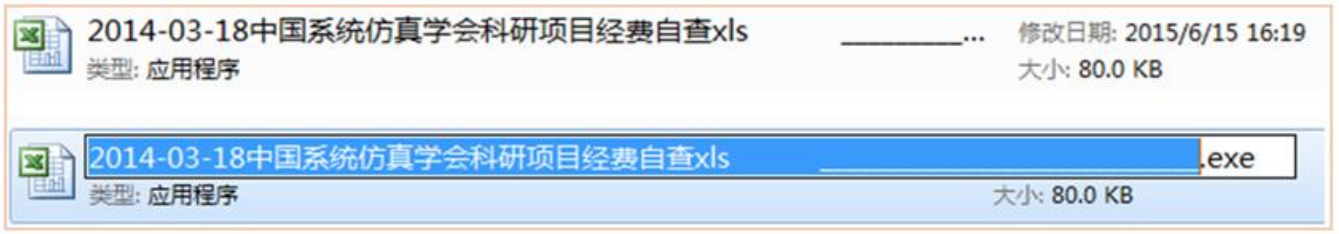


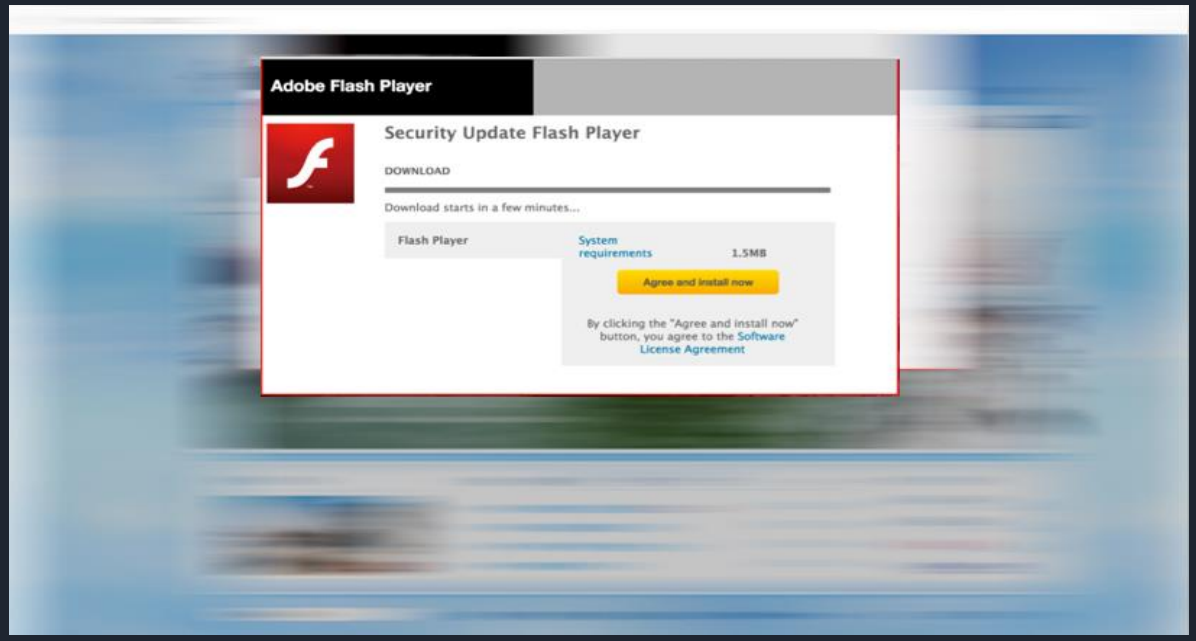
图 9 超长文件名和 excel 图标（白海豚组织）

APT攻击介绍-水坑

- “水坑攻击”,黑客攻击方式之一，顾名思义,是在受害者必经之路设置了一个“水坑(陷阱)”。最常见的做法是,黑客分析攻击目标的上网活动规律,寻找攻击目标经常访问的网站的弱点,先将此网站“攻破”并植入攻击代码,一旦攻击目标访问该网站就会“中招”。

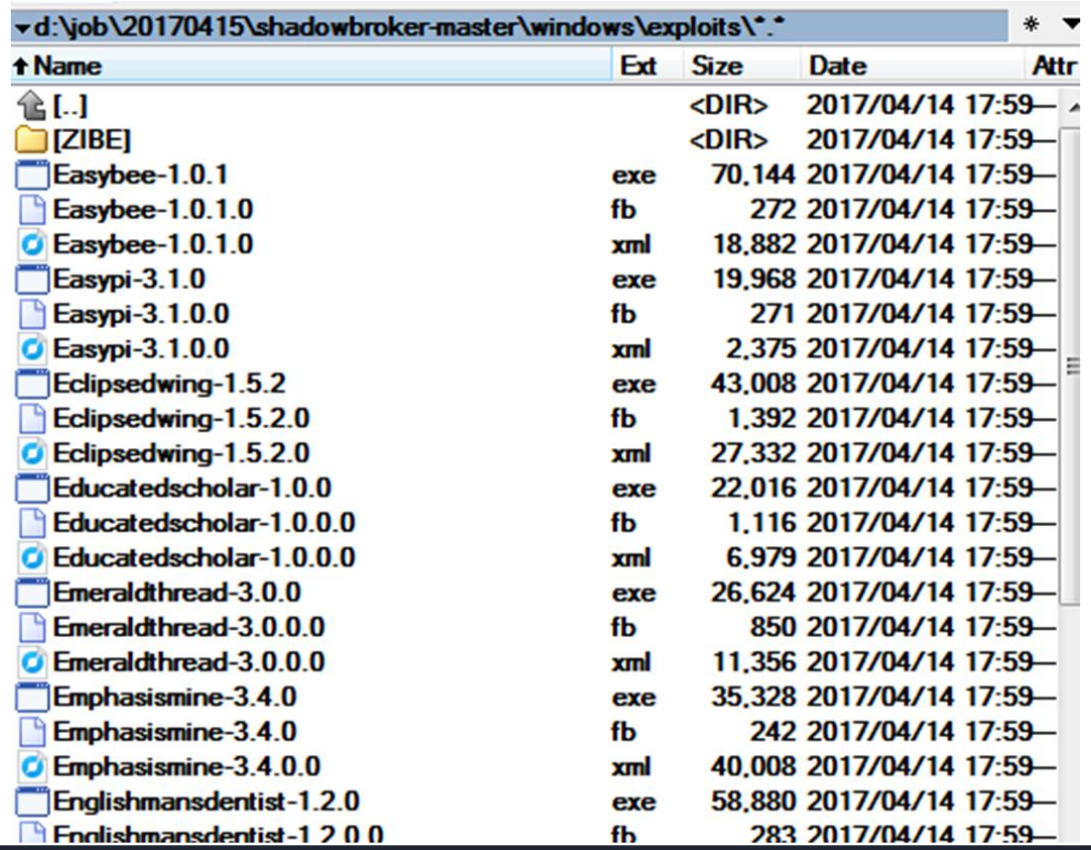
APT攻击介绍-水坑

OceanLotus组织首先通过渗透入侵的方式拿下某机构的文档交流服务器的控制权，在后台在“即时通”和“证书驱动”的正常安装文件上捆绑了自己的木马程序，用户下载安装驱动或RTX工具时，木马都有机会得到执行。攻击还在页面中插入了JS代码，用户访问时会弹出提示更新Flash软件，但实际提供的是伪装的Flash升级包，用户如果不小心下载执行就会中招 。



安全攻击方式介绍-NSA武器库

ShadowBroker 爆出 Equation Group 网络武器 （ FuzzBunch ）



供应链污染

定义：

供应链污染是在软件供应链中的各个环节利用不同的技术对软件进行污染。

1.源码编写

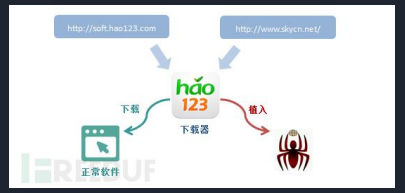
以思科公司为代表的科技巨头利用其占有的市场优势在科技产品中隐藏“后门”，协助美国政府对世界各国实施大规模信息监控，随时获取各国最新动态。

2.源码编译

XcodeGhost污染原理就是软件应用在编译过程中被强制加入了恶意的库文件。

XcodeGhost事件中，使用被污染Xcode开发的恶意APP 数量超过四千个，包括用户群非常庞大的QQ、微信、滴滴打车等应用，受害用户近一亿人

3.分发下载



用户使用hao123下载器下载软件的同时，下载器会在后台静默释放和执行一个名为nvMultitask.exe的释放器，进而向用户电脑植入恶意代码。即使用户不做任何操作直接关闭下载器，恶意代码也会被植入。

4.软件更新

攻击者利用水坑攻击，首先入侵ICS（Industrial Control Systems，工业控制系统）软件供应商主站，污染正版软件升级包，以ICS软件供应商为跳板来实现对 ICS的攻击，在ICS下载安装升级包的同时，Havex文件得以成功进入 ICS 内部。

供应链污染-XShell官方软件实例

2017年8月7日，NetSarang公司发布公告称其 7月18日发布的Xmanager、Xshell 、Xftp和Xlpd等多个产品存在安全漏洞，建议用户停用相关版本的产品，并及时更新至8 月5日发布的最新版。

存在后门的XShell等程序会在启动时发起大量请求DNS域名请求，并根据使用者系统时间生成不同的请求链接（见附件），其中 7月的相关域名为ribotqtonut.com，而8月的相关域名为nylalobghyhirgh.com 。
在这段时间使用过 Xshell等产品的用户信息有极大可能已被攻击者窃取。

在7月 23日至31日使用过相关Xshell等产品的用户信息 极有可能已被攻击者窃取，由于其他时间段内C&C无任何DNS解析，且NS服务器指向正常，信息被窃取的可能性较小，但不排除攻击者在后续过程中再次修改配置实施攻击。