2017 年度安全报告
——IoT 安全威胁

Iot Security

IoT 安全方向讨论

IoT 威胁分析

- IoT 不安全通信
- IoT 恶意软件威胁
- IoT 设备网络测绘情况

IoT 安全发展展望

Internet of Things Security

近年来，物联网技术的普及和快速发展让越来越多设备智能化，在公共领域，智慧环境（家庭，办公，工厂）领域，个人和社会领域等方面都有深入应用，新的技术和设备引入也带来了新的安全和隐私风险。该报告将探讨 2017 年整年关于 IoT(Internet of Things) 设备相关的安全问题。

通过对市面设备的分析和已爆发的 IoT 安全事件回顾，我们观察到以下问题。

安全漏洞：安全漏洞是一个必然存在的问题，但必要的安全开发规范和习惯会减少漏洞的产生。

不安全通信：很多现有成熟的安全功能设计是可以复用到 IoT 设备中的，但依旧存在以下不安全通信的问题。

- 未经认证的通信
- 未加密的通信
- 验证授权问题
- 缺乏必要的网络隔离

数据泄露：很多物联网设计方案依托于云端， 设备和云端处理通信，也会设备之间互相通信，均可能存在数据泄漏风险（用户信息，隐私， keychain 等）。

- 云端泄漏：云端服务面临传统云安全挑战， 但因为和物联网的融合， 一旦云端沦陷， 将影响接入的物联网安全
- 设备之间泄漏

开发设计安全意识：由于开发设计阶段人员安全意识不足， 导致设备原生就存在安全弱点， 易被攻击。

- 硬编码问题：由于开发过程不规范， 导致私钥， API KEY， 链接服务端密码被硬编码到固件， 导致信息泄露所带来的安全问题
- 默认身份认证凭据（密码，口令）：许多 IoT 设备使用相同的默认密码， 且用户无法主动修改密码

完整性和签名校验：对于 IoT 设备来说， 完整性校验和签名校验可以有效的对抗漏洞利用， 涉及到从 BootLoader 到 OTA 的各个阶段， 甚至可以到网络通信过程。

- 易感染恶意代码
- 易被篡改功能通信实现 IoT 设备本身的恶意行为
- 获取敏感信息，隐私等

IoT 设备的严重碎片化：由于 IoT 暂时属于新生事物， 各个厂商有不同的设备功能， 实现， 版本， 难免出现众多安全问题。

- Nday 重复利用：同一厂商的不同产品由于实现类似功能时复用代码， 有可能已披露的漏洞在某一产品修复但依然可以攻击另一产品
- 不安全的第三方：引用不安全的第三方库引发对自身产品的安全影响

硬件安全：IoT 设备一定会涉及嵌入式设备硬件， 硬件本身安全性也应考虑其中， 如串口， 一旦缺乏必要的认证机制， 暴露给攻击者， 攻击者可以很容易查找到敏感信息， dump 固件， 从而导致上述任意一环安全问题。

由这些安全问题， 整个 IoT 生态也爆发了一系列安全事件曝光于眼前， 也有大量没有曝光， 依旧暗藏于互联网空间中。

Mirai 及其变种： 2016 年爆发的 Mirai 事件经过一年的沉淀， 依旧对互联网产生着影响， 尤其是作者公开源代码后， 各种 Mirai 变种 " 百花齐放 "， 不少变种比 Mirai 原本更具有攻击性。

IoT_reaper: IoT_reaper 脱胎于 Mirai， 但在诸多方面更是优于 Mirai， 放弃弱口令攻击模式， 转而直接对 IoT 设备进行漏洞利用。

Satori: Satori 同样源于 Mirai， 除了在利用漏洞方面青出于蓝胜于蓝外， Satori 还有自扫描模块， 更加方便蠕虫的传播

Hajime: Hajime 和 Mirai 不同的是， 这是一个低调的 P2P botnet， 产生后并没有在公众视野过于张扬， 只是藏于暗处闷声发财， 由于是一个 P2P botnet， 安全人员很难通过黑名单对 Hajime sinkhole。

IoT 挖矿： 随着匿名货币龙头 BTC 的暴涨， 整个匿名数字货币水涨船高， 其匿名， 安全， 无法追踪的特性， 给网络黑产滋生带来了春天， 从今年 5 月的 SambaCry 漏洞后， 我们观察到大量野外利用攻击 IoT 设备进行 CPU 算力货币挖掘 (XMR 门罗币)，IoT 设备的数量优势以及漏洞修复推送不及时等原因让其成为挖矿黑产里的新贵。

DDoS: 无论是 Mirai 还是变种或任意 IoT botnet， 其变现要么挖矿， 要么 DDoS。

带来的变现能力和攻击能力更是不能小觑， 2016 年的 Mirai 事件就是最好证明。

IoT 安全方向讨论

IoT 设备所直面的安全和隐私风险挑战最终会在用户使用设备时完全体现， 由于 IoT 设备比传统的 PC 设备或服务器设备更加贴近用户态， 关联到的隐私数据或财产数据比传统设备更多， 这也使得攻击者青睐于这一新兴事物；其次， IoT 设备通常不会提供清晰完整的控制部署文档， 也不会告知再部署设备时有可能带来的风险， 这使得用户对设备完全处于黑箱状态， 当安全和隐私收到威胁时感知度不高。

· 用户心态

大多用户都是非技术人员或者对技术不感兴趣的群体， 这样的最终用户不具备评估隐私和安全的专业能力， 所以导致弱口令泛滥， 版本不升级等情况。

· 互联网接入

大量暴露在公网的 IoT 设备， 带来了恶意软件和漏洞利用的落地入口。

· 设备基数

IoT 设备由于大部分价格成本较低， 所以数量庞大， 大量的 IoT 设备基数也就使得易被攻击的比例增多， 数量庞大的设备能带来的变现能力和攻击能力更是不能小觑， 2016 年的 Mirai 事件就是最好证明。

· 易攻击性

许多 IoT 设备都不遵循安全性的最佳实现， 这使得攻击 IoT 设备门槛变低， 单带来的影响却变高。

· 设备功能特性

很多 IoT 设备贴合用户隐私， 如摄像头， 麦克风， 门锁， 医疗设备， 智能穿戴支付等， 和用户贴合越密切， 越容易泄露敏感信息， 偷听， 偷窥， 远程打开门锁， 盗刷支付等。

这一部分我们会针对不同切入点从技术角度讨论 IoT 的安全性，并将通过回顾 2017 一整年事件作为表现方式。

IoT 威胁分析

这一部分我们会针对不同切入点从技术角度讨论 IoT 的安全性，并将通过回顾 2017 一整年事件作为表现方式。

IoT 不安全通信

在厂商与厂商的合作之间势必会相互开放接口或者通信密钥以及一系列相关资源，这就导致了，但凡有一家合作厂商的安全做的不够出色，这就导致了短板效应的出现而拉低了众多厂商的安全等级。A 厂商和 C 厂商的合作使得 A 厂商几乎只承担的了集成 SDK 的成本就获得了一项智能家居产品，而 C 厂商也仅仅是提供了 SDK 就拓宽了自己的销售渠道，这样的合作模式肯定受到双方欢迎的，但是这之间的安全问题是值得关注的。

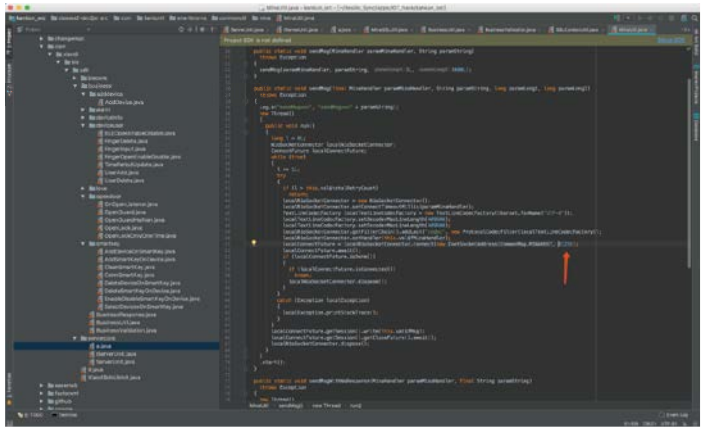
- 通信的密钥
- 身份 TOKEN
- 完整的设备信息
- 完整的控制请求

根据上述的问题，再结合一定的分析往往就能很容易的得出一份令人满意的漏洞。

认证绕过导致接管设备

智能硬件的人机交互很多由 APP 控制，如果 APP 存在安全问题，这就会导致许多隐患：

- 通信模型设计不当
- 验证认证流程存在绕过，或极不完善
- 查询接口权限认证粗糙
- 涉及服务器敏感信息泄露



逆向某智能家居 APK

通过简单的认证流程模拟，由一个手机号即可获取大量设备关键信息，甚至控制密码。

```
→ ~ java -jar /home/r7/IdeaProjects/ssl_kankun/target/ssl_kankun-1.0-SNAPSHOT.j
ar downShortcutDevice 1810471362
{"res":{"des":"成功","method":"downShortcutDevice","code":"success"},"datalist":
[{"id":2355932,"devPassswd":"s5zkV:vr","devType":"60","deviceName":"klight","use
rId":"1810471362","deviceMac":"18-fe-34-d0-d5-b3"},{"id":2355933,"devPassswd":"g
n.j;uCn","devType":"4","deviceName":"Smart plug","userId":"1810471362","deviceMa
c":"28-d9-8a-8d-3d-61"},{"id":2355934,"devPassswd":"nopassword","devType":"305",
"deviceName":"Universal remote control","userId":"1810471362","deviceMac":"28-d9
-8a-8d-3d-61#rc_1505200733"},{"id":2355935,"devPassswd":"SYLbgMM3","devType":"10
","deviceName":"智能摄像机","userId":"1810471362","deviceMac":"camera#6034b71eef
79093b#SYLbgMM3#10"},{"id":2355936,"devPassswd":"","devType":"72","deviceName":"
```

通过手机号获取设备信息

再根据已掌握的信息，进行设备控制指令的生成也是十分简单，进而完全控制设备。

```
In [1]: mini.device_open()
encryption:1/gjsQ5UlE1S9Coix6Pvo5EMZU9RFwWH9wpB5IGgLcqZWNZdQcOepO0ZeHPAil1h6FuaO
1Ro18BL3+Wjk2rfr7piTT40RknT1Jhw05GBrxM=

In [2]: mini.device_close()
encryption:1/gjsQ5UlE1S9Coix6Pvo5EMZU9RFwWH9wpB5IGgLcqZWNZdQcOepO0ZeHPAil1hQnymy
O8nR5NL/mbmAm/FQSGR22RGZgHUMu5vdqIuGyw=

In [3]: mini.red_control_pad(0, pad_button_command='open')
------------------------------
Universal remote control universal rc_1505200733
b'wan_phone%015bee58-8e09-4ec8-9710-31598127b4c2%gn.j;uCn%operate#3031#emit#rc_1
505200733#1505200736%uart\x00\x00\x00\x00\x00\x00\x00\x00'
encryption:1/gjsQ5UlE1S9Coix6Pvo5EMZU9RFwWH9wpB5IGgLcqZWNZdQcOepO0ZeHPAil1hhoQBS
84HBs284y0iy3nSLj9qgVbKm0N/bodO0GfFtcyPG65phjExUXXju33oPi//ZCTe5fQm4+i3V6Y8MRBSI
A==
        button 0: Switch 1505200736 open
```

完全控制设备

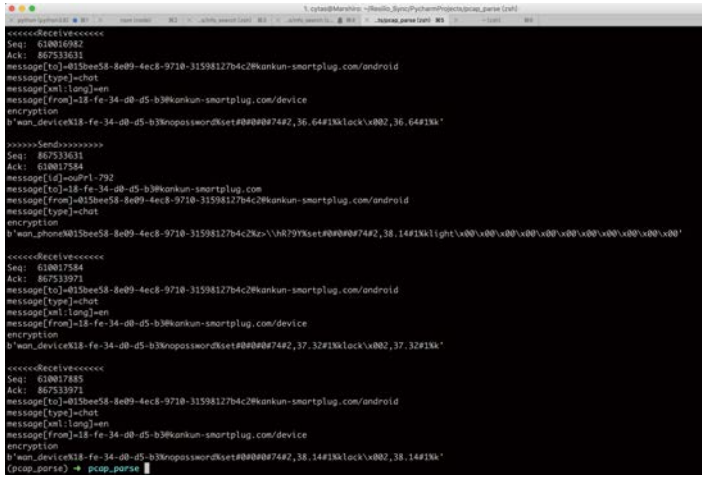
在远程控制解决方案上，互联网层面多由 XMPP 协议进行通信，但部分厂商在使用上仅仅着手于 XMPP 协议的及时性和开放性，对于一些必要的安全措施并没有进行良好的设计。

某厂商该特意设计了一个控制服务器，来接受和记录设备的绑定以及设备状态查询的服务，该服务器没有任何权限设置，也没有 token 校验，可以抓包后任意重放，从而获得任意设备 mac 所绑定的用户手机号，同时，还有以下安全问题：

- 在服务器上存储用户设备控制密码
- 对设备控制权限变更无校验，任何人可以在任何情况下对设备进行重新绑定，解绑，添加信任用户等危险操作
- 并在特殊的构造下，可以直接获取到任意设备的控制密码

在通信过程中消息内容采用固定格式：
wan_phone%015bee58-xxxx-xxxx-xxxx-31598127xxxx%password%open%relay

在局域网内设备采用 UDP 无连接通信，通过向设备发送连续 UDP 报获取设备信息，通过构造控制指令，变换 mac 地址即可批量完全控制设备。



小结

由于设备不安全通信，攻击者对现有用户会产生用户敏感信息泄露和 IoT 设备为攻击者大开方便之门的安全问 题。最终甚至危害到广大用户的人生以及财务安全。

已有的改进

- 尽量避免了将设备直接暴露在公网中
- 已有一些通信上的加密措施，不再是任何人都可以向设备发送消息
- 避免 IoT 设备的固件开发下载

尚存或演进的问题

- 以 CS 模式通信，但是通信结构和验证过程过于简单或没有，导致一旦攻破便可危害所有 在网设备
- APP 的安全开发意识十分薄弱
- 厂商合作之间的信任链单一，信任关系简单
- 多模式设计下，短板效 应明显，在某一模式安全性的缺失则导致整套安全系统崩溃
- 对用户信息，设备的存储和查询，存在致命的缺陷，对用户信息无任何保护手段，很容易获得设备用户的对应关系

早期，网络病毒、蠕虫入侵的对象只是计算机，随着物联网时代的到来，入侵的对象由电脑转向网络摄像头和 路由器．万物互联时代的恶意软件猖獗，导致 IoT 僵尸网络的疯狂滋生。

此处我们会讨论 2017 年几个极具代表 性的 IoT 恶意软件。

IoT 恶意软件威胁

2016 年爆发的 Mirai 事件经过一年的沉淀，依旧对互联网产生着影响，尤其是作者公开源代码后，各种 Mirai 变 种”百花齐放”，不少变种比 Mirai 原本更具有攻击性．

IoT_reaper

以 2017 年 10 月爆发的 IoT_reaper 为例，该僵尸网络脱胎于 mirai, 但是在诸多方面比 mirai 更进一步，特别是开始放 弃弱口令猜测，完全转向利用 IoT 设备漏洞收割。

IoT_reaper 相较于 mirai 仍有几个明显区分点：

1、恶意代码投入时不再使用弱口令猜测、而是使用 iot 设备漏洞，扫描发现效率大大提高；

2、恶意代码中集成了 LUA 执行环境，从而支持通过 lua 脚本编写复杂的攻击指令；

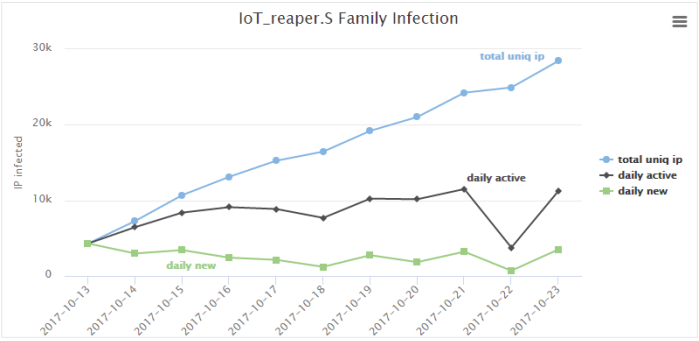
3、主动抑制了扫描速度，被安全研究者发现的风险大大降低。

其中最为可评说的是 IoT_reaper 完全放弃了 mirai 中利用弱口令猜测的方式，转为利用 IoT 设备的漏洞植入，当前 样本中集成了了 9 个 IoT 设备漏洞。

vulnerabilities	desc	source or Credit	release date	first seen in samples
1	D-Link 850L Multiple Vulnerabilities	Zdenda, Peter Geissler, Pierre Kim	2017-08-08	early than 2017-10-10
2	multiple vulnerabilities on multiple device	Pierre Kim	2017-03-08	early than 2017-10-10
3	vulnerabilities on JAWS			early than 2017-10-10
4	Netgear ReadyNAS Surveillance Unauthenticated Remote Command Execution	Kacper Szurek	2017-09-27	early than 2017-10-10
5	Vacron NVR Remote Command Execution	independent researcher	2017-10-08	early than 2017-10-10
6	Unauthenticated command execution on Netgear DGN devices	roberto () greyhats it	2013-05-31	2017-10-12
7	Multiple Vulnerabilities in Linksys E1500/E2500	m1k3	2013-02-05	2017-10-12
8	Multiple Vulnerabilities in D'Link DIR-600 and DIR-300 (rev B)	m1k3	2013-02-04	2017-10-12
9	multiple vulnerabilities on AVTech devices	Trietptm-on-Security	2016-10-11	2017-10-16

IoT_reaper 利用漏洞情况

在 2017.10.13 至 2017.10.23 之间单台 C2 的感染情况如下：



单台 C2 感染情况（数据来源于 360 网络安全研究院）

Satori

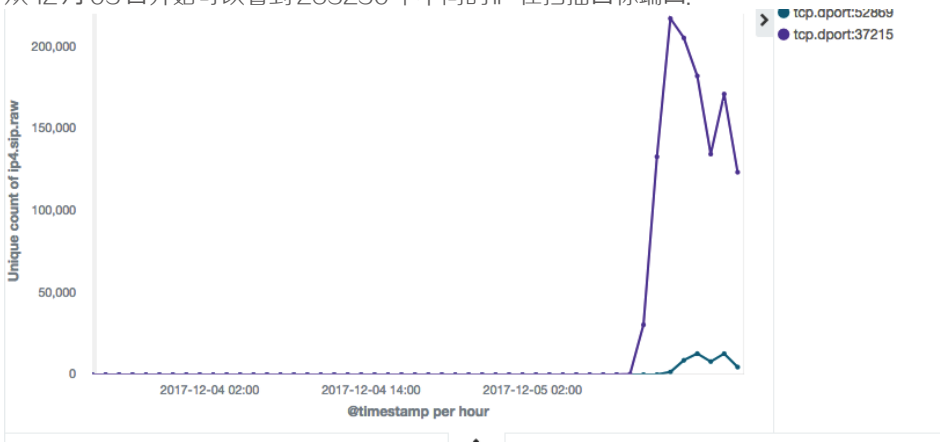
2017 年 11 月 22 日，360 网络安全研究院观测到有大量扫描集中在 23 和 2323 端口，并通过 admin/CentryL1nk admin/QwestM0dem 两组用户名密码进行爆破，其针对的是 ZyXEL 调制解调器，之后该僵尸网络 C2 被 sinkhole。

2017 年 12 月 05 日，Satori 的新版本开始在端口 37215 和 52869 上迅速传播。

相较于 mirai, 区分如下：

- bot 不再完全依赖以往的 loader/scanner 机制进行恶意代码的远程植入，而是自身有了扫描能力；
- bot 中增加了两个新的漏洞利用，分别工作在端口 37215 和 52869 上

从 12 月 05 日开始可以看到 263250 个不同的 IP 在扫描目标端口：



12 月 5 日目标端口扫描情况

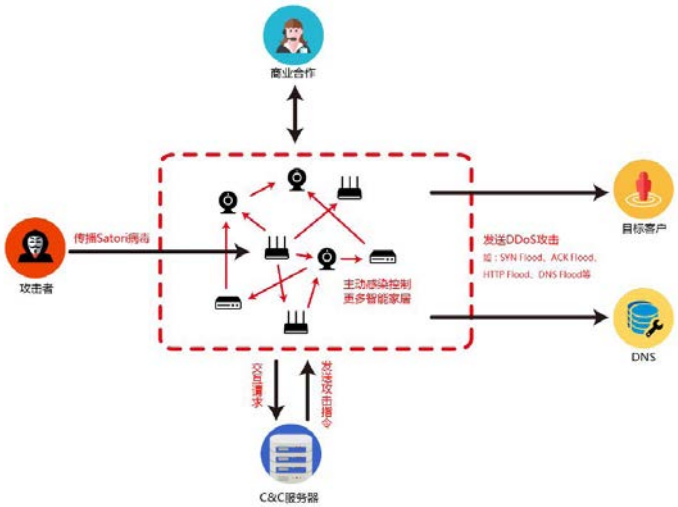
此次 Satori 的新版本主要利用到的是 CVE-2014-8361(52869 端口）和一个华为路由器的 0day CVE-2017-17215(37215 端口）。

Satori 在传播过程中，不仅会利用上述漏洞利用，而且会迫使受感染设备从原始下载 URL 处继续下载 Satori 自身的恶意代码。这样周而复始，使得恶意代码类似蠕虫式地传播。

Setbox

2017 年 8 月，国内观测到一系列 DDoS 攻击，通过溯源发现攻击来自于一批电视机顶盒，通过样本分析，依旧可以归为 mirai 家族的 Satori 变种，其 DDoS 攻击代码一致，代码结构基本没改变。但该僵尸网络针对有线电视终端机顶盒进行 telnet 口令爆破，将 mirai 的攻击面延展到机顶盒设备，这无疑增加了影响范围。

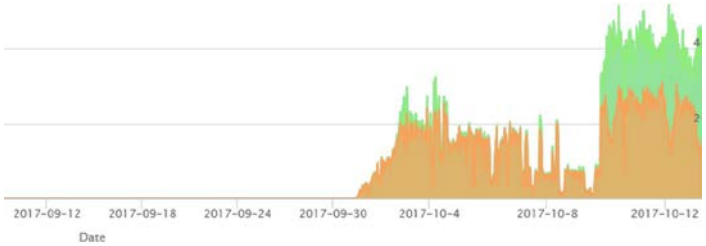
该僵尸网络攻击传播如图所示：



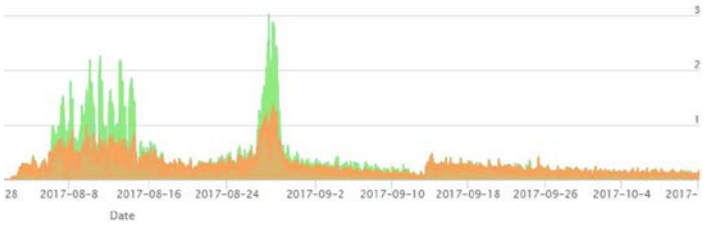
Satori 僵尸网络船舶原理

通过 360 网络安全研究院数据观测，两个 C2 请求态势如下：

185.130.xxx.xxx:7723



185.47.xx.xxx:8716



小结

由以上三个 IoT 恶意软件看出，在 Mirai 开源代码后，其变种层出不穷，且青出于蓝胜于蓝，主要表现为：

- 保留 Mirai 的基本框架特性
- 利用漏洞（甚至 0day）收割未被弱口令命中的 IoT 设备
- 自身添加了扫描能力
- 集成 LUA 环境升级自身编码能力
- 和安全研究人员对抗性加强

在物联网相关的安全问题越来越引发关注的背景下，对在互联网上暴露的 IoT 设备进行分析和梳理是非常有必要的，360CERT 自行研发的 QUAKE 网络测绘平台孕育而生，利用网络空间测绘技术，发现存储相关的 IoT 设备，形成威胁情报。

IoT 设备网络测绘情况

IoT 设备网络测绘总览

由于不同厂商设备指纹凌乱特征区分不明显，搜索结果可能和实际情况有出入，实际暴露情况可能比以下数据更多。

从全球分布来看，设备暴露情况以路由器为主，超过了 3100 万。

路由器全球测绘情况

其次为是视频监控设备，超过 800 万设备暴露在公网。

监控设备全球测绘情况

其中打印机位列第三，超过 80 万打印机暴露于公网。

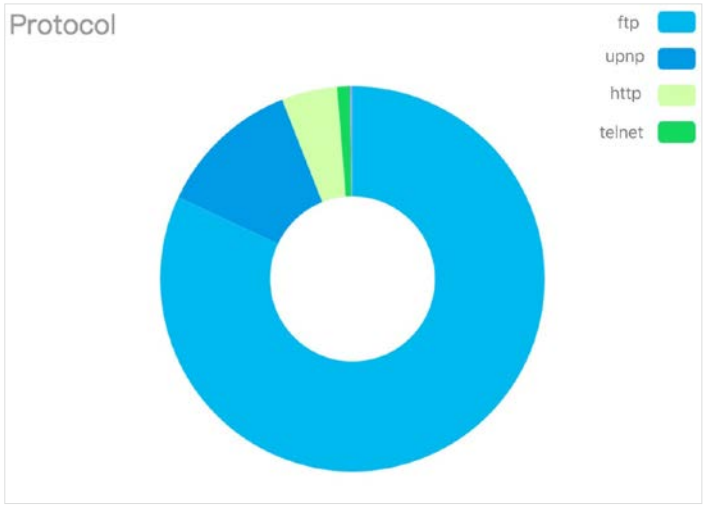
打印机全球测绘情况

路由器暴露情况

通过统计，我们发现一个有趣的情况，在路由器暴露全球分布上，中国独占鳌头总量超过 1000 万。

全球范围内，暴露数量最多的服务依次是 HTTP、FTP、UPnP 和 TR-069; 国内范围内，83% 的路由器开放了 UPnP 服务。

- HTTP 服务以 80, 8080, 8081 等常见端口为主
- FTP 服务端口为 21, 不排除存在匿名访问的情况
- TR-069 协议以 7567, 4567 端口为主
- Telnet 以 23 和 2323 为主，很多可以直接访问到魔改前后的路由系统，也由此 Telnet 成为攻击者的主要目标
- 从国内数据统计来看，超过 80% 的路由设备开放了 UPnP 服务

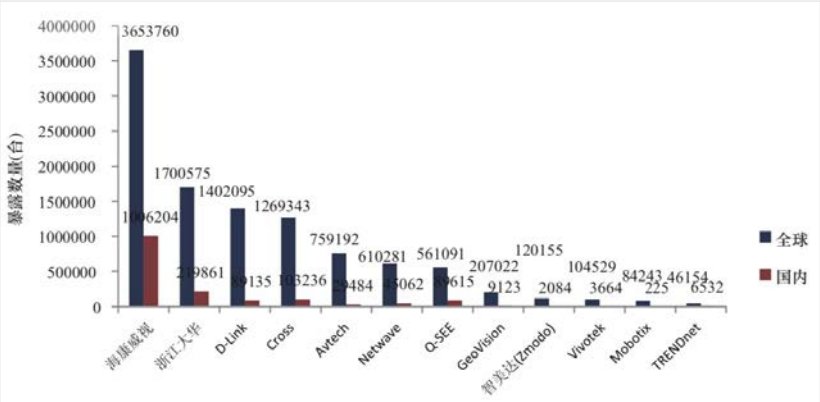


视频监控设备暴露情况

视频监控设备一直在安防领域占据主导地位，但今年发生的一些黑天鹅事件已经对智能安防设备的安全性敲响了警钟。

海康威视和大华两大厂商作为监控设备龙头，市场占有量大，所以暴露在公网的设备也以这两大厂商为主。

海康达到 300 万左右的全球设备暴露量，大华达到 200 万左右的全球设备暴露量，剩下以 D-Link, Cross 等厂商设备为主。



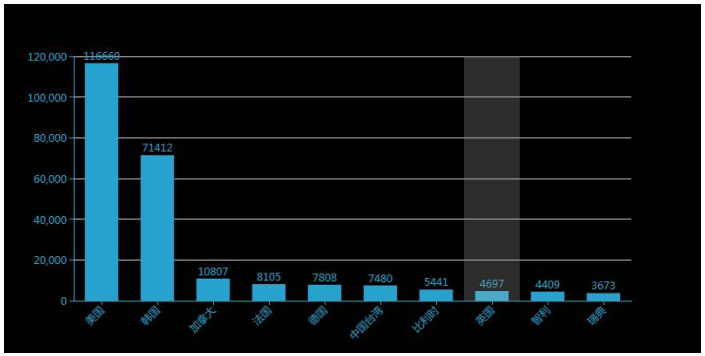
（该图表数据来自于绿盟＜物联网安全研究报告＞）

打印机设备情况

在本次统计中，令人意想不到的是打印机暴露占比不少，随着智能化办公的推进，移动设备打印需求增大，打印机逐渐朝着智能化发展，越来越多的功能也伴随而来更多的攻击面。

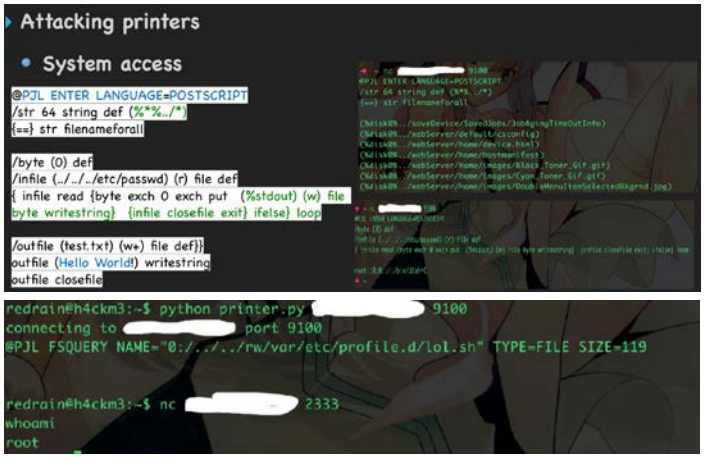
在全球设备暴露方面，惠普占量最多，达到 50 万左右，其次爱普生，富士施乐等大厂商也占比较高。

惠普打印机全球以美国暴露量最大，其次为韩国，加拿大。



在打印机寻求攻击面上，除了常规的 web 控制端，631 端口 ipp 访问弱口令一类认证问题，我们还发现了 9100 端口 PJL 服务安全问题。

通过 PJL 命令，可以使支持 Postscript 的打印机切换至 Postscript 模式，直接执行 Postscript 代码进而控制整个打印机。



小结

虽然一个物联网设备暴露在互联网并不一定意味着这个设备存在问题，但能说明该设备存在被攻击甚至被利用的风险。

通过网络测绘，我们发现以下问题：

- IoT 设备暴露公网量巨大，且很多存在安全风险
- 路由器和智能安防设备占有量为主
- 中国在全球设备暴露量中占比较大
- 大量的 IoT 设备暴露给攻击者落地进一步攻击提供了便携
- 越来越多的传统设备在向智能化靠近且已经占到全球设备暴露量前列

IoT 安全发展展望

合规性管理

IoT 正在驱动着一轮新的行业变革，但在不同行业，安全需求不统一，落地的安全方案也不全面成熟，在安全监管和应对措施上也没有明确思路。仅仅依靠某个组织，行业的安全推动是远远不够的，需要更高层级的协调以及统一的合规性管理。

举例参考 2016 年由于 Mirai 引发的断网事件，美国次月即发布了《保护物联网策略准则 (1.0 版)》，今年 5 月还签署了总统令《加强联邦网络和关键基础设施的网络安全》，均要求各私营企业、研究机构、社会团体围绕减少僵尸网络威胁和维护物联网终端设备安全问题，提出法律、政策、标准、技术等方面的建议 .。

加强政府的监管和立法，不仅有助于提高社会和国家对物联网安全的重 视程度，而且也能进一步推进物联网产业向着健康、安全的方向良性发展。

物联网安全标准建设

在任何技术的发展和演进过程中，标准都有着至关重要的作用，理论形成标准，标准指导产品和解决方案的完善。

从现在的情况看来，IoT 处于起步蓬勃发展的阶段，以指南和框架为主，能够指导产业落地，解决大块的安全痛点。

参考

http://blog.netlab.360.com/wa-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869/

http://blog.netlab.360.com/iot-reaper-a-quick-summary-of-a-rapid-spreading-new-iot-botnet/

http://www.nsfocus.com.cn/upload/contents/2017/12/20171205171653_35944.pdf

关于 360CERT

360CERT 全称“360 Computer Emergency Readiness Team”，我们致力于维护计算机网络空间安全，是 360 公司基于“协同联动， 主动发现， 快速响应”的指导原则，对重大网络安全事件进行快速预警、应急响应的安全协调团队。

微信公众号

新浪微博