浙江大学 360 校园版定期安全简报（2015 年 6 月）

一、 360 虚拟服务器全网等级情况

目前，浙大使用了 2 台服务器为 360 天擎校园版的服务器，一台总控中心，一台分控中心。

1.1 服务器安全等级概况：

1) 10.203.2.93

2) 10.203.2.92

截止至 2015 年 5 月 25 日 9 点止，10.203.2.92 为 360 的总控中心，只负责分发漏洞补丁事宜，安装客户端 5 台，10.203.2.93 服务器安装客户端 250 台。

1.2 受感染用户前 10 名（总排行 2015 年）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名
1	MMWL107-760	192.168.107.108	4541	VPN
2	zju	10.15.83.72	2812	玉泉-图书馆
3	PC-201309181536	10.189.253.139	1173	紫金港-无线网
4	DELL-PC	10.78.49.49	373	紫金港生科院
5	xugangjiang-PC	10.189.251.190	331	紫金港-无线网
6	fine	10.75.0.123	165	紫金港农生环大楼
7	YeZhiguo	10.71.123.36	119	紫金港-医学院综合楼
8	Zhang-PC	192.168.11.146	118	VPN
9	zju-HP	10.51.120.163	90	之江-主楼
10	user-PC	10.75.40.25	87	紫金港农生环大楼

1.3 受感染用户前 10 名（本月排行）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名	处理措施
1	MMWL107-760	192.168.107.108	4541	VPN	清除成功
2	107-PC	10.79.20.189	88	紫金港东一	清除成功
3	633B-PC	192.168.1.100	58	VPN	清除成功
4	wangfei-PC	10.15.42.87	44	玉泉-热能所	清除成功
5	YeZhiguo	10.71.123.36	30	紫金港-医学院综合楼	清除成功
6	zhaoyunyi	10.15.101.182	15	玉泉-图书馆	清除成功
7	Dell-PC	10.78.49.49	14	紫金港生科院	清除成功
8	lenovo-PC	10.189.164.104	14	紫金港-无线网	清除成功
9	zju-HP	10.51.120.163	12	之江-主楼	清除成功
10	OEM-20130419PJY	10.13.34.126	10	玉泉教十-五楼	清除成功

二、 安全简讯

2.1 11 月检测统计

- 360 天擎自 10 月初部署以来，随着每天的人数的增多，漏洞补丁、木马、系统危险项日益增多，本月所有统计如下表所示：10.203.2.93

日期	终端总数	活跃终端	体检分数	漏洞	木马	插件	系统危险项	安全配置项
2015-06-24	250	135	88	178	26	7	45	9
2015-06-23	248	186	59	53	16	7	34	9
2015-06-22	246	119	56	2	7	1	13	9
2015-06-21	246	98	50	0	7	2	13	9
2015-06-20	248	103	52	2	7	3	12	9
2015-06-19	251	185	57	2	15	7	27	9
2015-06-18	243	187	61	11	16	9	36	9
2015-06-17	243	177	63	0	19	8	33	10
2015-06-16	241	180	60	122	20	6	28	9
2015-06-15	240	181	61	109	18	8	30	9
2015-06-14	240	110	45	0	5	2	10	9
2015-06-13	242	122	54	0	6	3	14	9
2015-06-12	246	185	60	1	15	6	31	9
2015-06-11	245	192	57	135	16	6	30	9
2015-06-10	249	196	58	7	13	6	35	9
2015-06-09	247	193	60	1	19	6	32	9
2015-06-08	244	189	59	75	17	6	34	9
2015-06-07	246	122	48	0	6	3	15	9
2015-06-06	246	127	47	11	8	4	18	9
2015-06-05	252	185	58	11	11	5	31	9
2015-06-04	258	195	56	11	11	6	37	9
2015-06-03	245	200	58	0	11	6	34	9
2015-06-02	249	186	60	0	10	6	24	9
2015-06-01	249	188	59	62	10	5	32	9
2015-05-31	251	117	50	0	1	4	8	9
2015-05-30	252	122	55	4	2	3	15	9
2015-05-29	253	178	59	3	11	6	25	10
2015-05-28	254	179	62	68	8	6	32	9
2015-05-27	255	185	61	9	5	6	32	9
2015-05-26	253	185	60	29	11	6	34	8

2015-05-25	251	184	64	12	13	5	36	8

10.203.2.92：

日期	终端总数	活跃终端	体检分数	漏洞	木马	插件	系统危险项	安全配置项
2015-06-24	5	3	82	0	46	1	2	0
2015-06-23	5	3	82	0	0	0	1	0
2015-06-22	5	3	82	0	0	0	1	0
2015-06-21	5	3	82	0	0	0	1	0
2015-06-20	5	3	82	0	0	0	1	0
2015-06-19	5	3	82	0	0	0	1	0
2015-06-18	5	4	62	0	0	0	1	0
2015-06-17	5	4	62	0	0	0	1	0
2015-06-16	5	4	62	0	0	0	1	0
2015-06-15	5	4	62	0	0	0	1	0
2015-06-14	5	4	62	0	0	0	1	0
2015-06-13	5	4	62	0	0	0	1	0
2015-06-12	5	4	62	0	0	0	1	0
2015-06-11	5	4	70	0	0	0	1	0
2015-06-10	5	4	41	0	0	0	1	0
2015-06-09	5	4	62	0	0	0	1	0
2015-06-08	5	4	55	0	0	0	1	0
2015-06-07	5	4	62	0	0	0	1	0
2015-06-06	5	4	62	0	0	0	1	0
2015-06-05	5	4	62	0	0	0	1	0
2015-06-04	5	4	62	0	0	0	1	0
2015-06-03	5	4	62	0	0	0	1	0
2015-06-02	5	4	62	0	0	0	1	0
2015-06-01	5	5	33	0	46	1	2	0
2015-05-31	5	5	49	0	46	1	2	0
2015-05-30	5	5	49	0	46	1	2	0
2015-05-29	5	5	49	0	46	1	2	0
2015-05-28	5	5	62	0	28	1	2	0
2015-05-27	5	5	49	0	28	1	2	0
2015-05-26	5	5	50	0	30	1	2	0
2015-05-25	5	5	33	0	0	0	1	0

- 2.2 XP 加固日志数据

2014 年 4 月 8 日微软对 XP 系统停止服务以来，360 盾甲对 XP 的安全，防护，系统加

固产生了至关重要的作用。

360 天擎校园版自 2015 年以来，5 月 25 日至 6 月 24 日累计修复 12074 条。


分组 全网 开始日期 2015-05-25 结束日期 2015-06-24 查询

日期	终端名称	IP地址	操作类型	操作说明	详细说明
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{9F1DD175-2515-
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统常用文件夹	注册表位置：HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统常用文件夹	注册表位置：HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{B07AEC25-2EBE-
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{16BB4083-CA75-
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{B07AEC25-2EBE-
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统常用文件夹	注册表位置：HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统常用文件夹	注册表位置：HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Ex
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{16BB4083-CA75-
2015-06-24 14:13:45	lab3211	192.168.1.101	自动允许	修改 系统关键COM组件	注册表位置：HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{9F1DD175-2515-
2015-06-24 14:06:20	20131010-1508	222.205.111.110	自动允许	修改 系统常用文件夹	注册表位置：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Exp
2015-06-24 14:06:20	20131010-1508	222.205.111.110	自动允许	修改 系统常用文件夹	注册表位置：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Exp
2015-06-24 14:06:20	20131010-1508	222.205.111.110	自动允许	修改 系统常用文件夹	注册表位置：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Exp
2015-06-24 14:06:20	20131010-1508	222.205.111.110	自动允许	修改 系统常用文件夹	注册表位置：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Exp
2015-06-24 14:06:20	20131010-1508	222.205.111.110	自动允许	修改 系统常用文件夹	注册表位置：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Exp

共12074条记录 1 2 3 ... 805 下一页 跳转

2.3 本月终端插件情况统计

本月来累计统计的插件情况如下：

插件名称	危险级别	终端数量	上报日期
腾讯应用宝附带功能组件	高	8	2015-06-23 13:17:04
百度地址栏搜索插件	高	5	2015-06-23 12:54:02
百度杀毒所附带的浏览器插件	高	3	2015-06-23 10:13:56
捆绑安装的工具栏按钮	高	2	2015-06-23 09:59:18
腾讯搜索插件	高	2	2015-06-15 13:47:28
潜在风险的浏览器插件	高	1	2015-06-23 10:40:40
雅虎助手&上网助手	高	1	2015-06-15 19:11:56
主页恶意锁定模块	高	1	2015-06-23 10:13:56
带推广标记的网址导航图标	高	1	2015-06-18 22:51:36
百度工具栏	高	1	2015-06-17 10:41:58
SOSO 工具栏	高	1	2015-06-23 13:17:04
捆绑安装的小广告图标	高	1	2015-06-18 22:51:36

2.4 Microsoft 2015 年 6 月安全更新

安全公告编号:CNTA-2015-0013

6 月 9 日，微软发布了 2015 年 6 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 Exchange Server 中存在的 45 个安全漏洞。

其中，2 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

下表所示为了微软本月安全公告详情（按严重性排序），更多情况请参阅微软的官方网站。

公告 ID	公告标题和摘要	最高严重等级和漏洞影响	重新启动要求	受影响的软件
MS15-056	**Internet Explorer 的累积安全更新程序 (3058515)** 此安全更新程序可修复 Internet Explorer 中的多个漏洞。如果用户使用 Internet Explorer 查看经特殊设计的网页，那么这些漏洞的最严重后果可能是允许远程执行代码。成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。	严重 远程执行代码	需要重启	Microsoft Windows、Internet Explorer
MS15-057	**Windows Media Player 中的漏洞可能允许远程执行代码 (3033890)** 此安全更新程序可修复 Microsoft Windows 中的一个漏洞。如果 Windows Media Player 打开恶意网站上托管的经特殊设计的媒体内容，那么此漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以完全远程控制受影响的系统。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。	严重 远程执行代码	可能需要重启	Microsoft Windows
MS15-059	**Microsoft Office 中的漏洞可能允许远程执行代码 (3064949)** 此安全更新程序可修复 Microsoft Office 中的多个漏洞。如果用户打开经特殊设计的 Microsoft Office 文件，那么这些漏洞的最严重后果可能是允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。	重要 远程执行代码	可能需要重启	Microsoft Office
MS15-060	**Microsoft 常见控件中的漏洞可能允许远程执行代码 (3059317)** 此安全更新程序可修复 Microsoft Windows 中的一个漏洞。如果用户单击经特殊设计的链接或指向经特殊设计的内容的链接 ,然后在 Internet Explorer 中调用 F12 开发人员工具 ,那么此漏洞可能允许远程执行代码。	重要 远程执行代码	需要重启	Microsoft Windows

MS15-061	**Windows 内核模式驱动程序中的漏洞可能允许特权提升 (3057839)** 此安全更新程序可修复 Microsoft Windows 中的多个漏洞。如果攻击者登录系统并运行特制应用程序，最严重的漏洞可能允许特权提升。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。	重要 特权提升	需要重启	Microsoft Windows
MS15-062	**Active Directory 联合身份验证服务中的漏洞可能允许特权提升 (3062577)** 此安全更新程序可修复 Microsoft Active Directory 联合身份验证服务 (AD FS) 中的一个漏洞。如果攻击者将经特殊设计的 URL 提交给目标站点，那么此漏洞可能允许特权提升。在特定情况下，此漏洞会导致经特殊设计的脚本没有得到正确清理，进而可能导致在查看恶意内容的用户的安全性上下文中运行攻击者提供的脚本。对于跨站点脚本攻击，此漏洞需要用户访问被侵站点，才能发生恶意行为。	重要 特权提升	无需重启	Microsoft Windows
MS15-063	**Windows 内核中的漏洞可能允许特权提升 (3063858)** 此安全更新程序可修复 Microsoft Windows 中的一个漏洞。如果攻击者将恶意 .dll 文件放置在计算机或网络共享上的本地目录中，那么此漏洞可能允许特权提升。攻击者随后需要等待用户运行可以加载恶意 .dll 文件的程序，以便获得特权提升。不过，在任何情况下，攻击者都无法强迫用户访问此类网络共享或网站。	重要 特权提升	需要重启	Microsoft Windows
MS15-064	**Microsoft Exchange Server 中的漏洞可能允许特权提升 (3062157)** 此安全更新程序可修复 Microsoft Exchange Server 中的多个漏洞。如果已经过身份验证的用户单击指向经特殊设计的网页的链接，那么这些漏洞的最严重后果可能是允许特权提升。攻击者无法强迫用户访问此类网站，而是需要诱使用户单击链接，方法通常是诱使用户单击电子邮件或即时消息中的链接。	重要 特权提升	无需重启	Microsoft Exchange Server

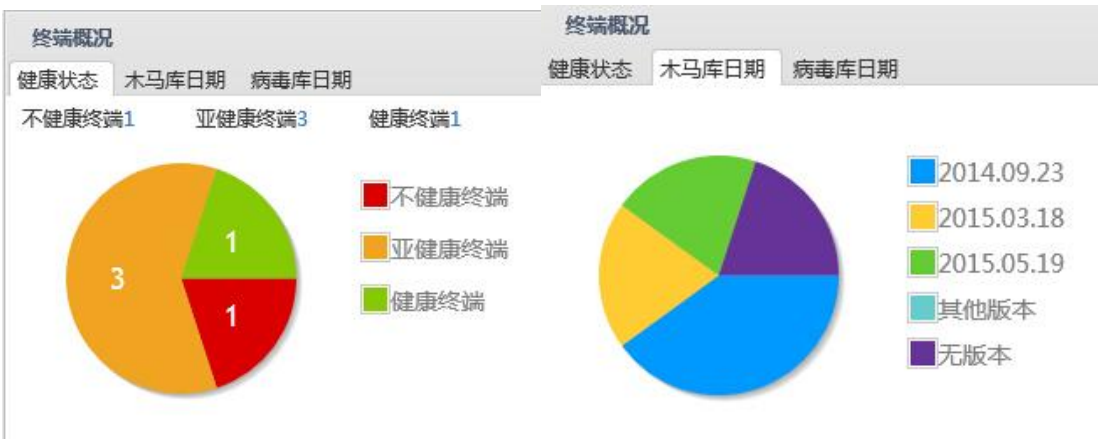
2.5 截止至本月月底的全网安全状况如下：

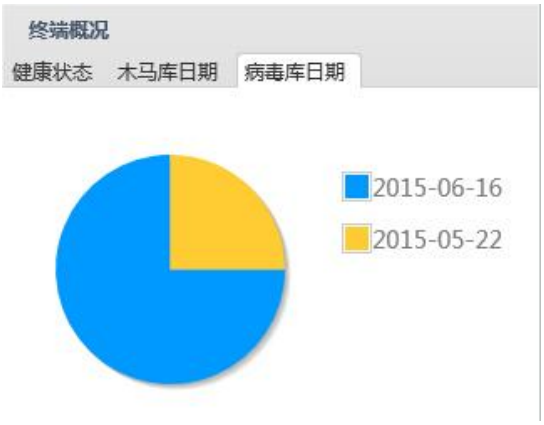
10.203.2.93　　10.203.2.92

2．6 终端概况如下

1）10.203.2.93

2）10.203.2.92





三、 免费的 WIFI 陷阱

今年 3.15 晚会上，最“任性”的安全问题当属被曝光的免费 WiFi 安全隐患。从安全工程师现场与观众互动的展示环节可以看出，大部分手机用户对于 WiFi 安全的认知还是一片空白。日前，360 手机安全中心发布《2015 中国 WiFi 安全绿皮书》，其中显示我国 80%的 WiFi 能在 15 分钟内轻易破解，甚至一位 7 岁的英国女孩看完网络视频教程后仅用时 10 分钟 54 秒便成功侵入一个 WiFi 热点。

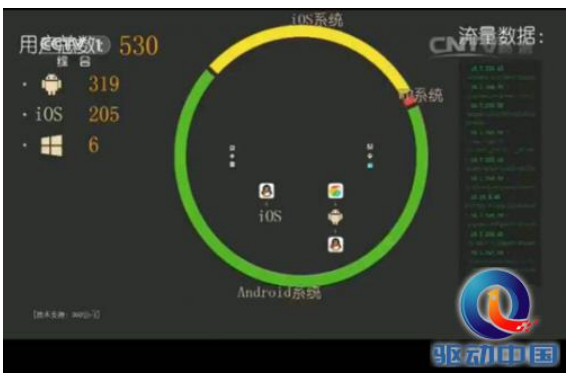


图 1：3.15 现场 技术人员展示利用危险 WiFi 搜集观众信息

有了 WiFi 就可以随时随地在社交软件上分享自己的照片， 3.15 晚会上主持人邀请大家连上大会现场设置的免费 WiFi 分享自拍照片。但是，免费的午餐真的免费吗？3.15 晚会舞台后的自动门开启，几位黑客亮相。原来，在大会现场不仅有节目组设置的正常 WiFi，同样还有黑客设置的虚假钓鱼 WiFi。

连接到虚假 WiFi 的观众，手机中的一切信息都已经被黑客所掌握。大会现场的屏幕上立即显示出有几台设备、什么手机设备连接了这个 WiFi。当然，观众发送的自拍照片也同样可以被截取，主持人甚至展示了这些观众手机中的邮箱账号以及密码信息。

其实，连接到虚假 WiFi 不仅仅是泄露邮箱账号及密码这么简单的问题。360 手机安全中心发布的《2015 中国 WiFi 安全绿皮书》总结出公共 WiFi 的三大安全隐患：1、在未知网络环境中，可能存在嗅探者，将我们的上网账号、密码等信息拿走；2、在未知网络环境中，可能存在 ARP 攻击（中间人攻击），导致文件、照片等私密数据被窃取；3、在未知网络环境中，可能存在 DNS，迫使上网者连接钓鱼网站，网银被盗刷等。

此外，《绿皮书》数据显示超五成的网友其实并不关心 WiFi 安全问题。在 Android 联网用户中有 49.75%的人会使用 WiFi 联网，在这其中，86.03%的人关注网速快慢问题、62.05 的人吐槽 WiFi 连接太麻烦，而对人们财产和个人信息构成威胁的 WiFi 安全问题，仅有 49.14%的人关心。

为了显示公共 WiFi 的危险性，一家 VPN 供应商曾雇佣了英国一位 7 岁小女孩来攻击公共网络。小女孩在搜索、观看了一个免费视频教程后，用时 10 分钟 54 秒便成功入侵了一个 WiFi 热点。而在网络上，相关视频教程多达上千万个。

360 手机安全专家称，3.15 晚会上的这一幕在我们的生活中其实并不陌生，只是真正意识到其危险性的人还太少。在诸多公共 WiFi 中，黑客可以在用户毫不知情的情况下引诱用户连入危险 WiFi。通过这样的方式盗取用户电话、电子邮箱账号及密码等信息，进而盗取网友银行卡存款的案例屡见不鲜。

因此，360 手机安全专家特别提醒用户在使用公共 WiFi 时需格外小心，夹杂在合法 WiFi 中的虚假 WiFi 用肉眼很难分辨。360 手机安全专家建议，尽量避免在连接公共 WiFi 的情况下登录邮箱或进行支付，同时可以使用 360 手机卫士，进行 WiFi 体检并打开支付专用安全通道，可以防 DNS 篡改、ARP 攻击等，保护网友上网及支付安全。

以上来源：驱动中国网(北京)

中新网 6 月 18 日电，昨日，央视《消费主张》报道了人们日常使用的无线网络存在巨大的安全隐患。在节目中，央视联合金山毒霸安全工程师在多个场景实际测验显示，火车站、咖啡馆等公共场所的一些免费 WIFI 热点有可能就是钓鱼陷阱，而家里的路由器也可能被恶意攻击者轻松攻破。网民在毫不知情的情况下，就可能面临个人敏感信息遭盗取，上网如同“裸奔”，访问钓鱼网站，会直接造成经济损失。

免费 WIFI 实为钓鱼诱饵 连接可致账户信息泄露

不久前，有媒体报道一位女子在麦当劳门前举牌抗议，使用公开 WIFI 上网被骗 2000 元，“连 WIFI 虽易，丢钱更易，且连且小心。”专家分析认为，该女子网购被盗的原因就很可能与 WIFI 钓鱼有关。

节目中，记者就与两位金山毒霸安全工程师进行了这样一场“钓鱼”实验。他们模拟黑客，在北京火车站和王府井商业区分别设置了名为 BEIJINGFREE 和 WANGFUJINGFREE 的两个免费 WIFI 热点，不设密码，作为“诱饵”引诱附近的网民连接。

由于该 WIFI 无需密码且信号较强，因此很快就有几十个网民通过手机、平板电脑、电脑等设备接入了这两个钓鱼热点，而网民在网络上的一举一动，甚至

其手机型号、打开的应用名称及上网信息，如浏览过的网页、机主 QQ 号码、微信朋友圈照片、淘宝、微博账号等信息，则同时被该 WIFI 创建者截获。

实验发现，在钓鱼 WIFI 环境下，网民若登录微博，黑客则利用网上存在的会话机制轻松劫持该网民的微博帐号，不仅可以以主人的身份浏览网民的私信内容和加密的相册，还可以进行发微博和删微博等操作。而如果网民接入 WIFI 后进行网购，那么黑客一样可以直接进入其网购账号，查看网民购买记录及个人联系方式、家庭住址等。

金山毒霸安全工程师赵昱表示：“WIFI 钓鱼热点其实就是在数据传输的上游设置了一道阀门，所有客户的数据都通过这个阀门与相应的网站进行传输，黑客通过一些特定的攻击设备，就可以对这些数据进行记录和抓取分析。这样，客户的相关信息就会被黑客获取。”

据了解，黑客所用的攻击设备在网上大量销售，而且成本很低，只需要几百元。它们的学习成本也不高，阅读一些使用说明就可以上手，一个电脑水平不高的人也可以在短时间内成为一名黑客。WIFI 钓鱼的成本越低，也就意味着普通网民面临的安全风险越大。

家用路由器易被攻克 专家：切记修改出厂密码

连接公共 WIFI 有风险，在自己家里使用路由器上网就安全吗？此次节目还实际演示了一次路由器劫持及网络欺诈过程。

据赵昱表示，黑客攻击家用路由器一般有三个步骤：第一，破解网民家里的 WiFi 密码；第二，接入 WIFI 之后，再破解路由器管理后台的账号和密码，获得路由器管理权；最后，在路由器中植入后门程序，窃取网民上网信息，或者篡改路由器 DNS 设置，使得网民在不知情的情况下访问钓鱼欺诈网站。

如节目所测试，被攻击的网民打开淘宝网站时，总会跳转到一个“淘宝 10 周年梦想创业基金活动”的官方网站。该网站提示网民输入淘宝账号、真实姓名、身份证号码、详细地址、甚至银行卡资料等一系列信息。如果网民稍不留意很难辨认出所谓的官方网站实为钓鱼网站。一旦按提示输入，那么用户隐私信息就会被黑客窃取，有可能威胁资金安全。

整个攻击过程仅需十分钟，普通网民可能根本感觉不到异常。更值得担忧的是，这些攻击方法早已成为了网上的热搜词。在网上搜索“WIFI 密码破解”，可以搜到约 300 万个结果，它们有的提供破解方法，有的提供破解软件，甚至还有讲解视频。这些本不该有的内容就成为普通网民路由器失守的关键。

金山毒霸安全工程师李铁军表示，多数网民缺乏一些相关的安全意识，路由器管理后台的初始登录账户和密码从不曾修改，这也给了恶意攻击者可乘之机。

五大 WIFI 安全使用建议为安全上网保驾护航

WIFI 是普通网民高速上网、节省流量资费的重要方式，虽然面临一些安全陷阱，但不可能因噎废食。金山毒霸安全工程师为此提供了五大安全使用建议。

第一，谨慎使用公共场合的 WIFI 热点。官方机构提供的而且有验证机制的 WiFi，可以找工作人员确认后连接使用。其他可以直接连接且不需要验证或密码的公共 WiFi 风险较高，背后有可能是钓鱼陷阱，尽量不使用。

第二，使用公共场合的 WIFI 热点时，尽量不要进行网络购物和网银的操作，避免重要的个人敏感信息遭到泄露，甚至被黑客银行转账。

第三，养成良好的 WIFI 使用习惯。手机会把使用过的 WIFI 热点都记录下来，如果 WiFi 开关处于打开状态，手机就会不断向周边进行搜寻，一旦遇到同名的热点就会自动进行连接，存在被钓鱼风险。因此当我们进入公共区域后，尽量不要打开 WIFI 开关，或者把 WiFi 调成锁屏后不再自动连接，避免在自己不知道的情况下连接上恶意 WIFI。

第四，家里路由器管理后台的登录账户、密码，不要使用默认的 admin，可改为字母加数字的高强度密码；设置的 WIFI 密码选择 WPA2 加密认证方式，相对复杂的密码可大大提高黑客破解的难度。

第五，不管在手机端还是电脑端都应安装安全软件。对于黑客常用的钓鱼网站等攻击手法，安全软件可以及时拦截提醒。金山毒霸正在内测的“路由管理大师”功能，还能有效防止家用路由器遭到攻击者劫持，防止网民上网裸奔。

以上来源：中国新闻网

四、 技术交流

欢迎老师和同学们前来交流问题，多提建议，希望下期简报内容更加接近大家的需求。

咨询服务电话：87951669

邮箱: netsafe@zju.edu.cn

工程师联系方式：

13588277982 章荣伟