FREEBUF

B…挪威居民医疗数据恐泄露；“文本炸弹”可使苹果 iM… 安卓恶意软件窃取Facebook凭证；广东省破获多起网犯…

82人围观 资讯

…花带雪红。闭阁寂寥常对此，江湖心在数枝中。

关注我们，分享每日精选文章

各位 Buffer 下午好，今天是 2018 年 1 月 22 日星期一（农历丁酉年腊月初六）。进了腊月就是年，BUF 早餐铺也然为大家带来可口早餐。今天份的早餐内容主要有：超过半数挪威居民的医疗数据恐遭黑客窃取；chaiOS “文炸弹” 可使 macOS 和 iOS 中的 iMessage App 崩溃；谷歌 Play Store 中再次出现恶意程序，可窃取 Faceboo登录凭证并推送广告；Triton 恶意软件利用施耐德电器设备中的0-day 漏洞发起攻击；Cloudfare 发布远程服务，替代 VPN 帮助企业解决安全问题；广东省公安部门 2017 年打击多起网络犯罪案件，侵犯公民信息、客攻击等案件榜上有名。

以下请看详细内容：

【国际时事】

超过半数挪威居民的医疗数据恐遭黑客窃取

1 月 的医疗机构 Health South-East RHF 表示其网站遭到入侵。该国卫生安全部门 He outh-East RHF 的异常流量，进而检测到入侵。据推测，这些异常流量就是黑客窃取 居

关注我们 分享每日精选文章

Health South-East RHF 管理挪威 9 个县（挪威一共 18 个县）的医疗单位，是挪威四大医疗保健区中最大的，为全国 290 万人提供医疗服务，超出挪威全体居民数目的一半。因此，如果入侵涉及到数据泄漏，对于挪威居民的影响比

挪威官方医疗为生部门在一份声明中表示：“已采取一系列措施应对威胁，未来将采取进一步措施。”

目前事件正在进一步调查之中。[来源：bleepingcomputer]

chaiOS “文本炸弹” 可使 macOS 和 iOS 中的 iMessage App 崩溃

研 OS 中出现 chaiOS “文本炸弹” bug，如果发送给其他用户，将导致该用户的 iMessa
应 示，这个 bug 影响了macOS High Sierra、iOS 10 到 10.3.3 以及 iOS 11 到 11.2.1 上的
iM

关注我们 分享每日精选文章

这个 bug 利用起来也很简单，只需向 web 页面发送一段可以发送信息的 JavaScript 代码即可。但是 iMessage 应用程
在处理这个代码时，出现了错误，最终出现应用程序崩溃，甚至进入重启循环。Bug 发现者在 Twitter 上分享了 Po
但因为担心会被滥用，该页面已经被屏蔽。

目前，这个 bug 主要是用作恶作剧，就像之前的微信发送 15 个句号就能造成卡顿崩溃一样。不过专家提醒，恶作剧要谨慎。因为之前有人恶作剧酿成大错，导致 Arizona 州的几个应急响应中心 911 服务崩溃，最终 19 岁的始作俑者临刑事指控。[来源：bleepingcomputer]

【漏洞攻击】

谷 意程序，可窃取 Facebook 登录凭证并推送广告

近 全研究人员在 Google Play Store 中发现了一种新的恶意软件 GhostTeam，影响到至 56 窃取 Facebook 登录凭据并向用户推送弹出式广告。GhostTeam 可以伪装成各种应用潜 具（如手电筒、二维码扫描仪和指南针）、提升性能的应用（如文件传输和清理器 和视频下载应用程序等。

安装之后，它首先会确认设备是否是仿真器或虚拟环境，然后相应地下载恶意软件有效载荷，促使受害者授予恶意序设备管理员权限，进而长久留存在设备中。随后，GhostTeam 会搜集设备专有 ID、定位、系统语言、显示参数等其中位置信息是从在线服务提供的 IP 地址获取的。

关注我们 分享每日精选文章

具体来说，只要用户打开 Facebook 应用程序，恶意程序会启动一个 WebView 组件，形成与 Facebook 类似的登录页面，并提示用户登录到 Facebook 重新验证帐户。WebView 代码会窃取受害者的 Facebook 用户名和密码，并将其发给远程黑客控制的服务器。也就是说，GhostTeam 使用传统的网络钓鱼手段来获取用户的登录凭证。

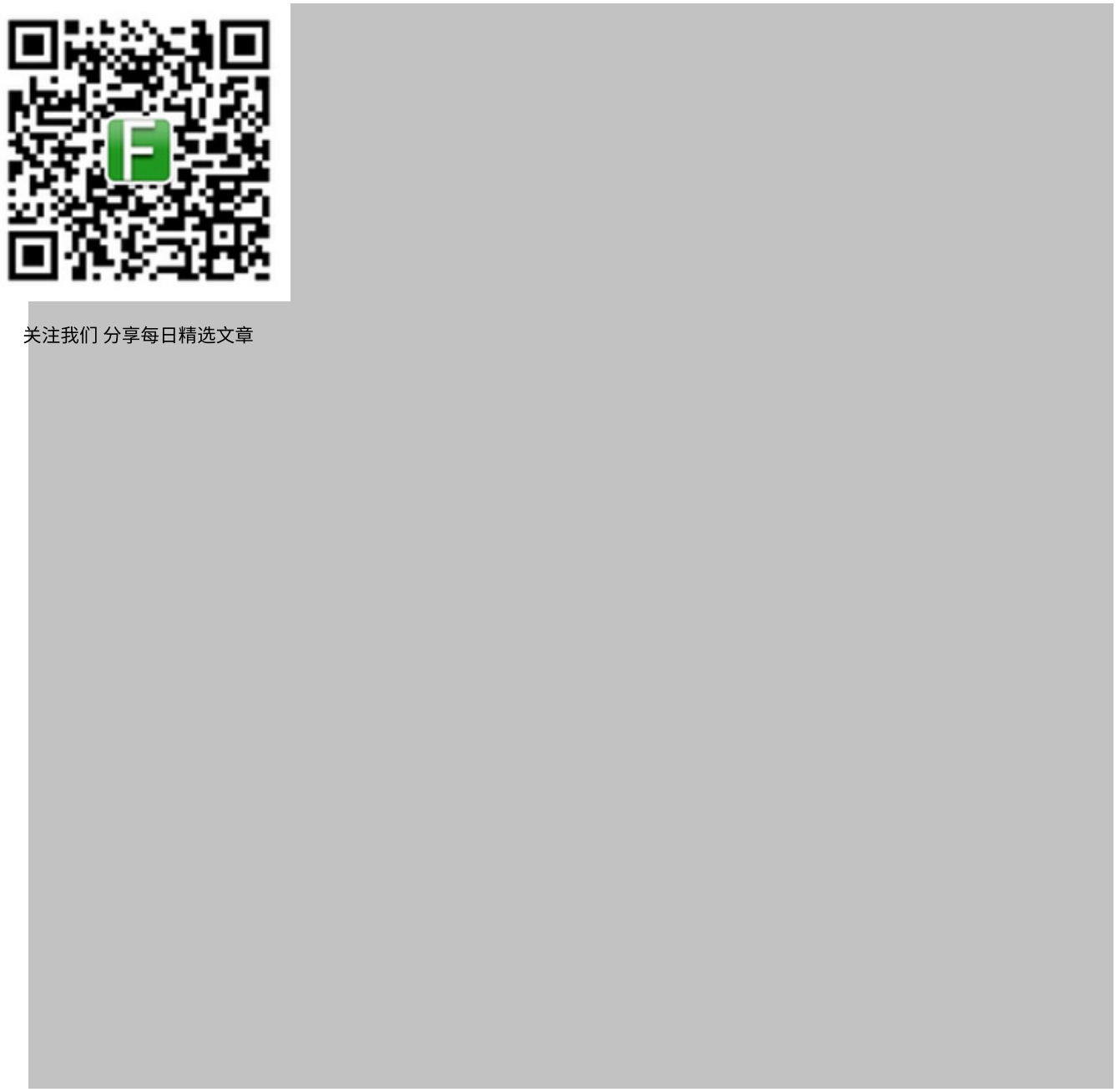
被盗的 Facebook账户可能会被用于传播更多恶意程序或形成社交媒体僵尸传播虚假新闻，还可能暴露“金融状况等其他个人身份信息”，并在在地下市场出售。除了窃取 Facebook 凭证外，GhostTeam 还会在后台激活设备推送弹出式广告。据研究人员介绍，受 GhostTeam 影响最多的用户分布在印度、印度尼西亚、巴西、越南和菲律宾。[来源：TheHackerNews]

Triton 恶意软件利用施耐德电器设备中的0-day 漏洞发起攻击

近日， Triton（Trisis）恶意软件利用施耐德电气 Triconex 安全仪表系统（SIS）控制器中的 0-day 漏洞,针对重要基

施耐德电气的 Triconex SIS 设备主要用于监控进程状态并将其恢复到安全状态；或者在参数显示存在潜在危险的情下，将进程安全关闭。恶意软件使用 TriStation 专有协议与 SIS 控制器进行交互，获取读写的程序和功能。

> 恶意软件可以扫描和映射工业控制系统，侦查 Tricon 控制器并发布命令。一旦入侵成功，Triton 就变成了一款远控木马（RAT），攻击者可以直接通过远程网络连接来控制系统。



施耐德电气表示：Triton 利用了旧版 Triconex Tricon 系统的一个漏洞，只影响到少数几个较旧的版本，而补丁将在来几周内发布。此外，他们也正在研发一种工具，用于检测并删除控制器上存在的恶意软件，预计将于下个月上市建议客户始终执行 Triconex 文档“安全注意事项”部分的说明，将控制器保持在锁定的机柜内，在设置为“PROGRAM”模式时显示报警。

工业网络安全和威胁情报公司 CyberX 表示，基于对 Triton 的分析，恶意软件是由伊朗开发的，针对的目标组织位

【行业动态】

Cloudfare 发布远程访问服务，替代 VPN 帮助企业解决安全问题

现如今，移动办公和云计算已经打破了安全边界，而企业 VPN 也已成为传统的解决方案。这两者都已经无法应对
边界或进入 VPN 的攻击者。Google 很早以前就认识到了这个问题，并将 BeyondCorp 作为边界和 VPN 替代品。
Be 的需求，专注于验证设备（提供、识别设备证书）及其用户，并在其应用程序周围
施 可信网络和不可信网络之间的区别，侧重于验证来自任意位置的认证访问。但是，
Be 。目前，Cloudflare 也推出了类似的服务 Cloudflare Access，相当于 BeyondCorp 模
的 工在公司网络之外工作，且无需使用 VPN。

Cloudflare 的专家表示：“VPN 会减慢工作速度。因为每次页面加载都会增加 VPN 服务器的额外往返次数。此外，

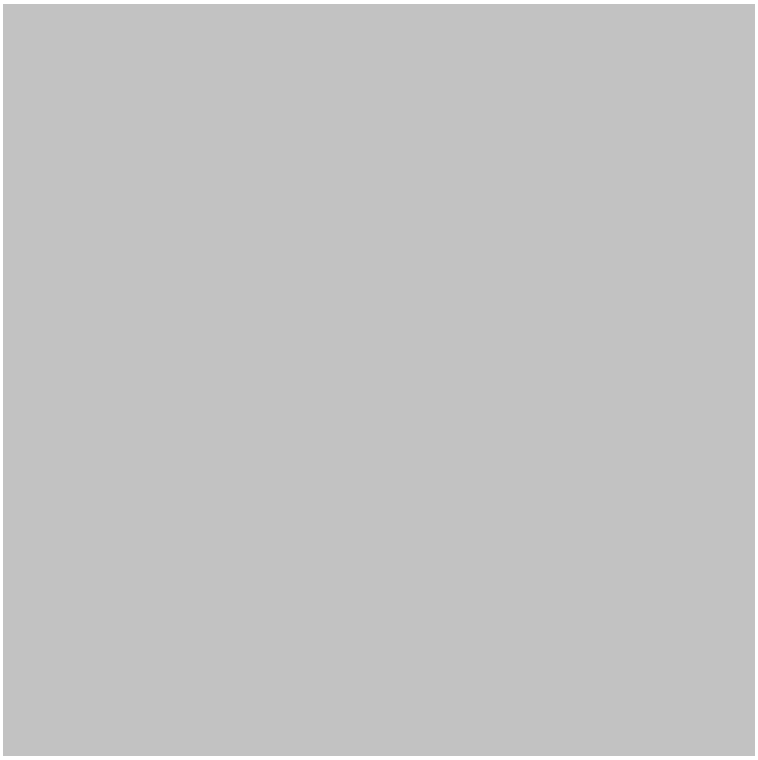
Cloudflare Access 相当于在不同的身份验证包装中保护客户的应用程序。确切来说，它保护的不是员工的设备而是
司的应用程序。“即使攻击者设法进入设备，公司网络的每个访问都被 Cloudflare 记录，客户（公司）可以监控异常
况。因此，在每个应用程序周围进行认证的模型不仅增加了攻击阻力，还提供了一个中央存储库，让安全团队可以
看异常情况，跟踪不良行为并快速做出响应。Cloudflare 服务的客户管理员将拥有每个员工设备的单一视图 – 当它
并使用每个不同的服务 – 以服务为基础，如果发生异常情况，管理员可以立即撤回用户的访问权限。

不 共企业设备，用户仍然需要自主负责远程设备的安全，建议用户在所使用的设备上
多 Week]

【

广 多起网络犯罪案件，侵犯公民信息、黑客攻击等案件榜上有名

广东省公安厅召开发布会，通报严打整治网络犯罪“安网2017”专项行动全年的战果以及“安网2018”专项行动计划，
公布了2017年度广东公安十大精品网络案件，其中多个案件创造全国第一，比如打掉网络攻击“黑产圈”排行第一的
罪团伙“暗夜攻击小组”。



据统计，2017年，广东警方共发起集群战役22次，破获网络犯罪案件4588起，抓获嫌疑人1.2万名，打掉犯罪团伙4
个，缴获被泄露、窃取、买卖的公民个人信息7.1亿余条，清缴木马病毒程序443个，查获钓鱼网站服务器236台，集
战役次数、规模以及破获案件数量等均创历史新高。

2017年，广东警方依托以波次打击、集群战役打击、跨国跨境跨区域打击为主要特征的打击网络犯罪“广东模式”，
拳打击侵犯公民个人信息、黑客攻击破坏等上游性源头性犯罪以及技术含量高的网络诈骗等新型网络犯罪。[来源：
民网]

上一篇：Meltdown/Spectre最新进展：补丁影不影响性能？英特尔做了一场实验
下一篇：漏洞暴露近一周才修复，某成人VR App可能泄露用户信息

选择文件 未选择任何文件

昵
请输入

必须 您当前尚未登录。登陆? 注册

邮
请输入

必须（保密）

关注我们 分享每日精选文章

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

AngelaY
LIE TO ME

119
文章数

59
评论数

最近文章

- BUF早餐铺 | 超半数挪威居民医疗数据恐泄露；“文本炸弹”可使苹果iMessage App崩溃；安卓恶意软件窃取Facebook凭证；广东省破获多起网络犯罪案件
  2018.01.22
- RubyMiner挖矿程序24小时内影响全球30%的网络
  2018.01.18
- BUF早餐铺 | 强力安卓恶意软件Skygofree分析发布；恶意Chrome扩展程序影响50多万用户；女博士被电信诈骗85万；腾讯帮助警方逮捕绝地求生作弊工具开发者

浏览更多

相关阅读

B… 者被…

B… anna…

B… 遭破…

B… 卓短…

B… ；据…

关注我们 分享每日精选文章

特别推荐

不容错过

OpenVAS开源风险评估系统部署方案

魅影儿 2017-04-30

双刃剑与灰色地带：“泄露数据收藏家”的素描

孙毛毛 2016-09-27

2015最酷的Hack方式有哪些？

【限时优惠】FreeBuf精品公开课 |

简单	2016-01-05	FB客服	2017-09-16

关注我们 分享每日精选文章