

## 为何要警惕“零点击”网络威胁

简译版

非官方中文译文·安天技术公益翻译组 译注

### 文档信息

原文名称	Why Zero-Click Cyberthreats Should Be on Your Radar		
原文作者	戴安娜·克特林格 (Diana Kightlinger)	原文发布日期	2020年7月2日
作者简介	戴安娜·克特林格是一位资深记者、撰稿人和博客作者，擅长科学、技术和医疗领域。		
原文发布单位	Security Intelligence		
原文出处	<a href="https://securityintelligence.com/articles/why-zero-click-cyberthreats-should-be-on-your-radar/">https://securityintelligence.com/articles/why-zero-click-cyberthreats-should-be-on-your-radar/</a>		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</li> <li>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</li> <li>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</li> <li>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。</li> </ul>		

## 为何要警惕“零点击”网络威胁

戴安娜·克特林格

2020 年 7 月 2 日

多年来，统计数据显示，人为错误是造成网络攻击的最大原因。我们一直在强调培训的重要性，以防止几乎不可避免的攻击。我们认为，防御网络威胁的关键是：防止毫无戒心的用户点击网络钓鱼邮件，从而防止恶意软件感染设备和系统。

现在，上述措施仍然很重要。但是，由于最近出现的“零点击”（zero-click）网络威胁，这些措施都将无济于事。“零点击”攻击不需要人为错误，甚至不需要人为干预。这类攻击取决于特殊格式的数据——例如用于电子邮件、SMS 消息、MMS 消息、语音消息和电话的数据，其代码会危害系统。易受攻击的系统通常是用于收发电子邮件和传递消息的通信平台，在确定邮件和消息是否可信之前，这些平台会先接收数据。

据 Wired 报道，网络犯罪分子非常青睐此类攻击，这是因为：“零点击”攻击无需目标点击诱饵，且交互更少，因此更不容易暴露。

### “零点击”攻击如何运作

ZecOps 公司发现的“零点击”漏洞揭示了此类威胁是如何运作的。该漏洞影响 iPhone 和 iPad 的 Mail 应用程序。ZecOps 发现，攻击者可以通过向目标邮箱发送精心制作的邮件来触发此漏洞。自 2012 年 9 月苹果公司发布装有 iOS 6 的 iPhone 5 以来，该漏洞一直存在。

当目标在 iOS 12 上的 MobileMail 应用中打开邮件，或者在 iOS 13 上发送邮件时，攻击者就能够利用此漏洞，通过占用大量内存的邮件远程感染设备。根据 ZecOps 的说法，邮件不必很大，只需占用足够的 RAM 即可。即使邮件未被下载完，该漏洞也可以被触发。

从 iOS 13 开始，用户在后台打开 Mail 应用时，此漏洞就会启动“零点击”攻击。然后，攻击者可以在 Mail 应用中阅读、编辑、泄漏或删除邮件。但是，攻击者将无法完全控制目标设备。因此，ZecOps 与苹果公司一致认为，要想发动攻击，攻击者需要利用其他信息泄露漏洞和内核漏洞。

苹果公司于 2020 年 4 月 16 日在 iOS 13.4.5 Beta 版中修复了该漏洞，但是该补丁在通用

版本中尚不可用。如果用户无法使用 Beta 版，则 ZecOps 建议禁用 Mail 应用，转而使用不易受攻击的 Outlook、Edison Mail 或 Gmail 等应用。但是，在补丁可用之前，攻击者可能会利用这个时间窗口来攻击尽可能多的设备。

## “零点击”攻击的隐患

iPhone 和 iPad 的“零点击”漏洞并非最近发现的唯一漏洞。SC Magazine 报道称，2020 年 1 月，谷歌 Project Zero 调查团队的安全研究员马特乌斯·尤尔齐克（Mateusz Jurczyk）发现了一个漏洞，该漏洞使攻击者能够利用 Android 图形库处理图像。为此，三星向其表示了感谢。在运行 Android 4.4.4 或更高版本系统的三星手机上，该漏洞能够启动“零点击”攻击。一旦攻击成功，攻击者将获得与手机所有者相同的权限，包括查看呼叫日志、联系人和 SMS 消息等。

据 The Defence Works 报道，2019 年 5 月，攻击者利用一个 WhatsApp 漏洞，使用该应用的语音通话功能拨打攻击目标的电话。即使攻击目标不接听电话，其手机上也会被安装恶意软件，之后该通话会被删除。呼叫者和接收者手机之间的互联网连接隐藏了包含软件代码的受感染数据包。之后，攻击者可以控制数据，包括呼叫日志、消息和位置，以及诸如摄像头和麦克风等功能。

另一起攻击涉及游戏、流媒体、笔记本电脑和某些智能家居设备中使用的 Wi-Fi 芯片组中的漏洞，Help Net Security 报道称。

这类攻击随着移动设备的普及而蓬勃发展。Statista 公司预测，到 2021 年，仅智能手机的数量就将达到 38 亿部。网络威胁利用了设备、网络覆盖和 Wi-Fi 漏洞，以及大量宝贵的数据。如今，很多人在手机中存储的个人和机密信息与在台式机中存储的一样多。

## 如何应对“零点击”攻击

Wired 表示，未能识别出大量的“零点击”攻击并不是由于相关漏洞少，而是因为此类攻击很难被发现。例如，受感染苹果设备的用户可能只会注意到手机邮件应用暂时出现速度下降或突然崩溃，而相关内容（邮件、消息或通话）不一定会保留在设备上。例如，ZecOps 指出，尽管数据显示目标 Apple 设备已接收了漏洞利用电子邮件，但邮件服务器上却没有这些邮件。

手机的一些安全特性设计，也很难检测“零点击”攻击。例如，由于 iMessage 的端到端加密，苹果或安全监控公司会发现，识别自定义的“零点击”消息非常困难。即使是最不复杂的攻击也几乎不会留下线索。崩溃日志可以作为查找异常（表明可能存在恶意活动）的好起点。

为了防止“零点击”攻击，需采取基本的网络安全措施，例如：及时更新所有设备上的操作系统、固件和应用程序；仅从官方商店下载应用并卸载不再使用的应用；提防安装新应用、下载未知文件或点击可疑链接的请求等。

使用口令保护设备，但要关闭自动 Wi-Fi 和蓝牙连接。不要越狱手机免费下载应用，因为这样会使 Apple 和 Google 提供的保护无济于事。

随着移动攻击面的扩大，“零点击”攻击越来越有欺骗性、危险性并不断发展。目前，我们需警惕“零点击”威胁，采取预防措施来保护移动设备并及时了解新型攻击。我们还应意识到，随着手机与计算机的区别越来越小，企业需要像对待台式机和笔记本电脑一样认真对待手机安全。

## 安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,始终坚持自主先进的能力导向,依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累,研发智甲、探海、镇关、捕风、追影、拓痕等系列产品,为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系,依托全面持续监测能力,建立系统与人员协同作业机制,指挥网内各种防御机制联合响应威胁,实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合,协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设,支撑起协同联动的实战化运行,赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方,全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴,目前,安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点,在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面,实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体(如 APT 组织)及其攻击行动,进行持续监测和深度解析,协助客户在“敌情想定”下形成有效防护,通过深度分析高级网空威胁行为体的作业能力,安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可,已连续六届蝉联国家级安全应急支撑单位,是中国国家信息安全漏洞库六家首批一级支撑单位之一,亦是国家网络与信息安全信息通报机制技术支撑单位,国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日,在习近平总书记主持召开的网络安全和信息化工作座谈会上,安天创始人、首席架构师作为网络安全领域发言代表,向总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了安天总部,并对安天人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问:

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问:

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>