Facebook发现APT黑客使用的新Android恶意软件

由 比尔·图拉斯 (https://www.bleepingcomputer.com/author/bill-toulas/) 八月 5，2022 上午10：40 0

Meta（Facebook）发布了2022年第二季度的对抗性威胁报告，其中的亮点是发现了两个网络间谍集群，这些集群与使用新的Android恶意软件的黑客组织“Bitter APT”和APT36（又名“透明部落”）相连。

这些网络间谍特工使用Facebook等社交媒体平台来收集情报（OSINT）或使用虚假角色与受害者交朋友，然后将他们拖到外部平台下载恶意软件。

今年早些时候，APT36和Bitter APT都被观察到在策划网络间谍活动，因此Facebook的报告为他们最近的活动提供了一个新的维度。

巴基斯坦国家赞助的演员APT36最近在一场使用MFA绕过工具 (https://www.bleepingcomputer.com/news/security/hackers-use-modified-mfa-tool-against-indian-govt-employees/)针对印度政府的运动中被曝光。

2022年5月还观察到了 (https://www.bleepingcomputer.com/news/security/bitter-cyberspies-target-south-asian-govts-with-new-malware/)Bitter APT，针对孟加拉国

政府使用具有远程文件执行功能的新恶意软件。

苦涩的**APT**使用新的安卓间谍软件

Meta的报告解释说，Bitter APT参与了针对新西兰，印度，巴基斯坦和英国目标的社会工程，使用了长时间的互动并投入了大量的时间和精力。

该组织的目标是用恶意软件感染其目标，为此，它使用了URL缩短服务，受感染站点和第三方文件托管提供商的组合。

“该小组积极回应我们检测和阻止其活动和域基础设施，”Meta在报告中评论道 (https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf)。

“例如，Bitter会试图发布损坏的链接或恶意链接的图像，以便人们必须在浏览器中输入它们而不是点击它们 - 所有这些都是为了逃避执法失败。

Bitter最近的攻击还揭示了威胁行为者武器库中以两个移动应用程序的形式增加的内容，分别针对iOS和Android用户。

iOS版本是通过Apple的Testflight服务提供的聊天应用程序，这是应用程序开发人员的测试空间。通常，威胁行为者通过将其呈现为“更安全”或“更安全”来说服受害者下载这些聊天应用程序。

Facebook发现的Android应用程序是一种新的恶意软件，Meta将其命名为“Dracarys”，它滥用可访问性服务，在未经用户同意的情况下为自己提供更高的权限。

从那里，它会将自己注入各种Android应用程序中，以充当间谍软件，窃取短信，安装应用程序和录制音频。

“Bitter将Dracarys注入到YouTube，Signal，Telegram，WhatsApp和自定义聊天应用程序的特洛伊木马（非官方）版本中，这些应用程序能够访问通话记录，联系人，文件，短信，地理位置，设备信息，拍照，启用麦克风和安装应用程序，”Meta的报告解释说。

Meta强调，Dracarys在所有现有的防病毒引擎上都未被发现，突出了Bitter创建隐形自定义恶意软件的能力。

APT36依赖于商用工具

APT36是一个不太复杂的威胁参与者，但仍然是一个强大的威胁，依赖于复杂的社会工程策略和现成的恶意软件。

Meta发现的最新活动针对阿富汗，印度，巴基斯坦，阿拉伯联合酋长国和沙特阿拉伯的人们，特别关注军事官员和人权活动家。

APT36的成员在Facebook上创建帐户，冒充欺骗性或虚构公司的招聘人员，并使用WeTransfer文件共享服务向目标发送所谓的工作机会。

下载的文件包含XploitSPY的修改版本，Meta将其命名为“LazaSpy”。参与者的修改包括地理限制定位机制的失败实现。

除了LazaSpy之外，APT36还采用了Mobzsar，这是一种商品恶意软件，使运营商能够访问通话记录，联系人列表，短信，GPS数据，照片和麦克风。

相关文章：

俄罗斯黑客使用伪造的DDoS应用程序感染亲乌克兰活动家 (https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-ddos-app-to-infect-pro-ukrainian-activists/)

Google Play商店中的Android恶意软件获得了200万次下载 (https://www.bleepingcomputer.com/news/security/android-malware-on-the-google-play-store-gets-2-million-downloads/)

Facebook广告推送Android广告软件，在Google Play上安装量为700万 (https://www.bleepingcomputer.com/news/security/facebook-ads-push-android-adware-with-7-million-installs-on-google-play/)

新的Android恶意软件应用程序从Google Play安装了1000万次 (https://www.bleepingcomputer.com/news/security/new-android-malware-apps-installed-10-million-times-from-google-play/)

LinkedIn网络钓鱼目标管理 Facebook 广告帐户的员工 (https://www.bleepingcomputer.com/news/security/linkedin-phishing-target-employees-managing-facebook-ad-accounts/)

人造人 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/ANDROID/)

容易 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/APT/)

苦 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/BITTER/)

网络间谍活动 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBER-ESPIONAGE/)

脸书 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/FACEBOOK/)

恶意软件 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MALWARE/)

(https://www.bleepingcomputer.com/author/bill-toulas/)

比尔·图拉斯 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/BILL-TOULAS/)

(MAILTO:BILL.TOULAS@BLEEPINGCOMPUTER.COM) (HTTPS://TWITTER.COM/BILLTOULAS)

Bill Toulas是一位技术作家和信息安全新闻记者，在各种在线出版物上拥有超过十年的经验。作为一名开源倡导者和Linux爱好者，他目前在关注黑客攻击，恶意软件活动和数据泄露事件以及探索技术迅速改变我们生活的复杂方式方面找到了乐趣。

PREVIOUS ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/GOOGLE-CHROME-NOW-BLOCKS-ALL-MICROSOFT-TRACKERS-MOST-OF-THE-TIME/)

NEXT ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/TWITTER-CONFIRMS-ZERO-DAY-USED-TO-EXPOSE-DATA-OF-54-MILLION-ACCOUNTS/)

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums/index.php?app=core&module=global&section=register)

You may also like:

热门故事

Twitter证实零日漏洞用于公开**540**万个账户的数据 (https://www.bleepingcomputer.com/news/security/twitter-confirms-zero-day-used-to-expose-data-of-54-million-accounts/)

DuckDuckGo浏览器现在大多数时候都会阻止所有微软跟踪器。

(https://www.bleepingcomputer.com/news/security/duckduckgo-browser-now-blocks-all-microsoft-trackers-most-of-the-time/)