2016 年 6 月 9 日，星期四

TESLACRYPT：战争已经结束

Talos 已完成对 TeslaCrypt 解密工具的升级工作，该工具现在可以应对此勒索软件变体的任何版本。您可以在此处下载该解密工具。

2015 年 4 月，Talos 首次对 TeslaCrypt 版本 1.0 进行了仔细研究，随即明确指出这种勒索软件的运行方式，以及如何开发相应的解密工具。不久之后，TeslaCrypt 出现了版本 2.0，对加密过程进行了完善，导致 Talos 发布的初版解密工具不再有效。

不过，一家安全研究机构发现了 TeslaCrypt 版本 2.0 中的漏洞。他们没有公开自己的发现，而是在不让攻击者知道其最新版勒索软件中存在漏洞的情况下，悄悄帮助用户解密文件。后来就像大家知道的那样，在 2016 年 1 月，TeslaCrypt 出现了版本 3.0。由此开始，一场猫鼠大战正式上演。

但是在短短几个月后，TeslaCrypt 勒索软件的作者于 2016 年 5 月出人意料地决定停止其活动，而且发布了解密主密钥。ESET 公司随即利用该信息制作并发布了 TeslaCrypt 版本 3 和版本 4 的解密工具。

勒索软件是一个不断发展的威胁，但是围绕 TeslaCrypt 的战争已经全面结束，因为我们有了适用于该勒索软件变体所有版本的解密工具。TeslaCrypt 从 2015 年初开始骚扰用户，在该勒索软件作乱期间，防御者与攻击者展开了互不相让的较量。为了帮助那些仍有文件被该勒索软件加密的用户，Talos 发布了一个适用于所有 TeslaCrypt 版本的解密工具。有关各个 TeslaCrypt 版本在加密上的缺陷，以及 Talos 解密工具的源代码，可在此处获取。

发布者：EARL CARTER；发布时间：15:50
标签：ALPHACRYPT、解密、TESLACRYPT