2017 年 9 月 20 日星期三

Beers with Talos 第 13 期：CCleanup 大事件、大显身手和漏洞攻击经济

Beers with Talos (BWT) 播客第 13 期现已上线。 下载本期播客并订阅 Beers with Talos：

ITUNES GOOGLE PLAY

如果您对 iTunes 和 Google Play 不感兴趣，不妨试试 Beers with Talos 播客：www.talosintelligence.com/podcast。

此播客侧重于安全研究主题，节奏明快，睿智而不乏幽默。面对这种不断快速演变的威胁形势，要想时刻把握安全主题的最新动态可谓困难重重。Beers with Talos 提供了很多安全要闻，简单易懂、生动有趣，无论是研究人员、高管，还是安全新手，都可以轻松理解要旨。

第 13 期亮点集锦：

Struts - 什么时候应该进行修补，什么时候应该积极彻底地进行修补。我们将以 Equifax 数据泄露事件为例，讨论修补如何帮助您改善安全，让您永远不必发出“可能发生在我身上”的后怕感慨。这个话题自然会引出以供应链入侵、CCleaner、Python 和 Nyetya 变种为关键词的本周最大事件。Avast 难辞其咎，但其实所有科技公司都很容易受到供应链攻击。那么，各公司可以采取哪些措施来保护自己？用户又能如何改善这方面的安全状态？结束这些话题后，我们还将讨论漏洞攻击经济，按供求关系来判断漏洞攻击的价值。Zerodium 有一份全面的价目表，我们如何使用经济学的基本知识来辨别各种漏洞攻击的可用性和难度？

第 13 期导听：

01:00 - 讨论会 - 今天您在想什么？
10:25 - Struts - 可能发生在我身上（但我们已进行修补）
19:20 - CCleaning 清理供应供应链
33:26 - 漏洞攻击经济
53:28 - 结论和零星想法

Talos Struts 文章：http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html 和 http://blog.talosintelligence.com/2017/09/apache-struts-being-exploited.html
Talos CCleaner 文章：http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
Zerodium 漏洞攻击价目表：https://www.zerodium.com/program.html
==========

主播：Craig Williams (@Security_Craig)、Joel Esler (@JoelEsler)、Matt Olney (@kpyke) 和 Nigel Houghton (@EnglishLFC)。
主持人：Mitch Neff (@MitchNeff)

查看所有节目：
http://cs.co/talospodcast

通过 iTunes 订阅（欢迎发表评论！）
http://cs.co/talositunes

查看 Talos 威胁研究博客：
http://cs.co/talosresearch

订阅威胁源新闻通讯：
http://cs.co/talosupdate

在 Twitter 上关注 Talos：
http://cs.co/talostwitter

对我们的主题提供反馈和建议：
beerswithtalos@cisco.com

发布者：MITCH NEFF；发布时间：10:37