2017 年 5 月 30 日

BWT 第 5 期 - 那些从“零日”开始就被滥用的词

Beers with Talos 第 5 期“那些从‘零日’开始就被滥用的词”现已上线

收听方式：

在 iTunes 上收听

直接在 Talos 播客页面收听。

本期内容：

节目组探讨了 WannaCry 攻击活动中暴露出的 Samba 的潜在问题，以及是否需要阻止 SMB 端口。（大家应该已经阻止该端口了，是吧？）节目中还讨论了一些历史教训，并针对如何正确使用“零日”、“后门”，以及业界为了提高点击率而大肆宣传或滥用其他术语提出了建议。

在本周的“畅所欲言”环节，我们将听到：Joel 正设法解决他的设计课题中存在的内在冲突；Nigel 的女儿偷窃了高端电子产品；Matt 作弄了美国某大城市的一线救援人员；Craig 了解到 JRE 沙盒是个万能药方；Mitch 为了逗大家开心发布了一条咄咄逼人的“道歉信”。

反馈问题：

是什么让 Joel 困扰不已？请通过我们的 Twitter 帐号 @TalosSecurity 给我们留言，不要忘了使用 #BWT 这个话题。（顺便问一句，#BWT 是什么意思？）

主题列表：

11:45 - Samba 以及为什么 Linux 蠕虫如此顽固，异常顽固。说真的，最好阻止端口 445。

22:56 - 要是不幸成为网络攻击的受害者，可以说是咎由自取

25:45 - 有时候根本无法打补丁

27:20 - 术语的真正含义 - 后门、零日等等

38:55 - 当你必须调整防御对象时，调整设置起不到太大作用。

引用链接：

Talos WannaCry 博文 - http://blog.talosintelligence.com/2017/05/wannacry.html

Talos Samba 博文 - http://blog.talosintelligence.com/2017/05/samba-vuln-details.html

Talos SSH 博文 - http://blog.talosintelligence.com/2015/04/threat-spotlight-sshpsychos.html

联邦新闻电台 - https://federalnewsradio.com/technology/2016/10/hackers-not-yet-pulling-big-guns-data-breaches-nsa-official-warns/

==========

本期嘉宾

Craig Williams、Joel Esler、Matt Olney 和 Nigel Houghton。

主办方

Mitch Neff。

查看所有节目

http://cs.co/talospodcast

通过 ITUNES 订阅

http://cs.co/talositunes（欢迎发表评论！）

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

欢迎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：14:42

分享此文