[网络安全自学篇] 六十九.宏病毒之入门基础、防御措施、自发邮件及APT28样本分析

原创

Eastmount 于 2020-04-21 22:19:09 发布 7223 收藏 33

分类专栏： 网络安全自学篇 APT分析及溯源 文章标签： 网络安全 宏病毒 APT分析 安全防御 Word

本文链接：https://blog.csdn.net/Eastmount/article/details/105646194

网络安全自学篇 同时被 2 个专栏收录

107 篇文章 2590 订阅 ¥19.90 ¥99.00

订阅专栏

APT分析及溯源

15 篇文章 49 订阅

订阅专栏

这是作者的网络安全自学教程系列，主要是关于安全工具和实践操作的在线笔记，特分享出来与博友们学习，希望您们喜欢，一起进步。前文分享了利用永恒之蓝漏洞加载WannaCry勒索病毒，实现对Win7文件加密的过程，并讲解WannaCry勒索病毒的原理。这篇文章将讲解宏病毒相关知识，它仍然活跃于各个APT攻击样本中，本文包括宏病毒基础原理、防御措施、自发邮件及APT28样本分析。基础性文章，希望对您有所帮助。

作者作为网络安全的小白，分享一些自学基础教程给大家，主要是关于安全工具和实践操作的在线笔记，希望您们喜欢。同时，更希望您能与我一起操作和进步，后续将深入学习网络安全和系统安全知识并分享相关实验。总之，希望该系列文章对博友有所帮助，写文不易，大神们不喜勿喷，谢谢！如果文章对您有帮助，将是我创作的最大动力，点赞、评论、私聊均可，一起加油喔~

文章目录

一.什么是宏

1.基础概念

2.安装配置

3.录制新宏案例

二.宏病毒

1.宏病毒基础

2.自动宏案例

3.宏病毒感染

三.宏病毒的自我保护与防御

四.案例：CDO