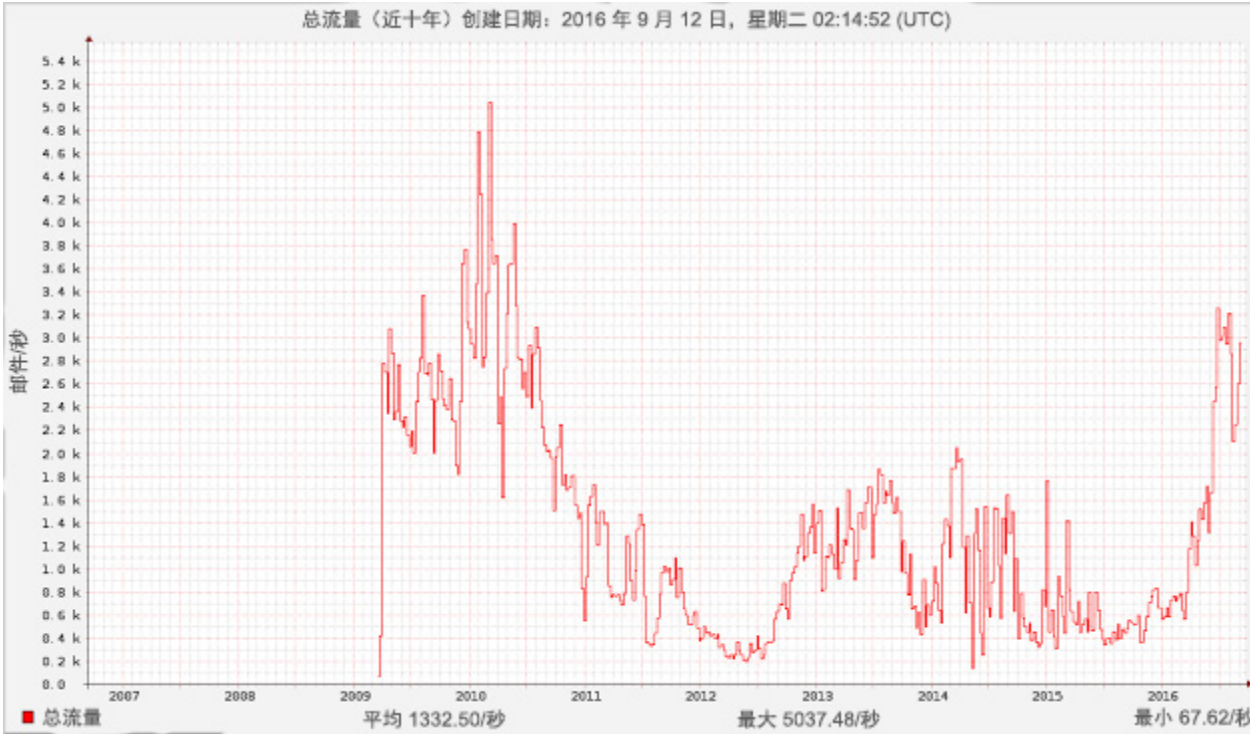
2016 年 9 月 21 日，星期三

垃圾邮件卷土重来

作者：Jaeson Schultz。

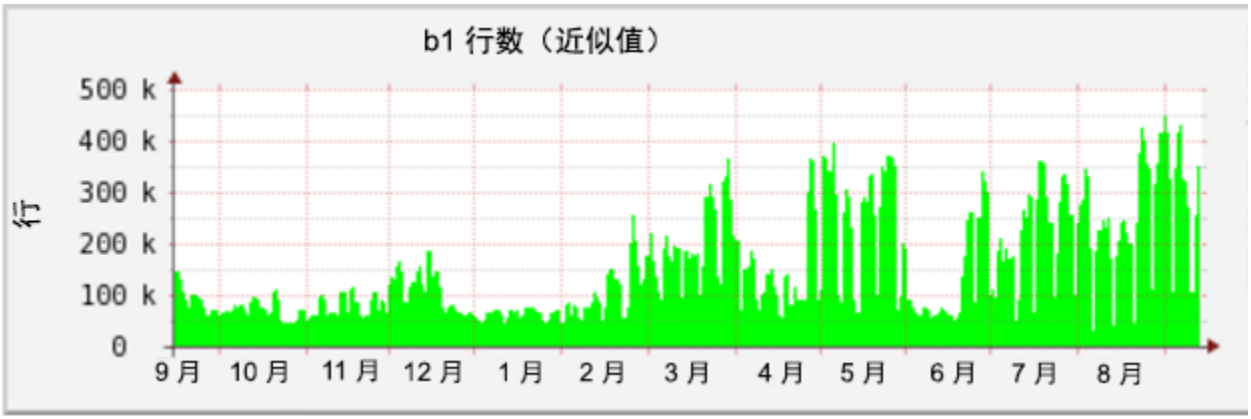
在过去五年中，垃圾邮件数量一直处于相对平静的状态。回到十年之交，世界曾遭遇创历史数字的垃圾邮件骚扰。然而，随着新的反垃圾邮件技术的发展，加上一些成功摧毁垃圾邮件相关僵尸网络的举措，垃圾邮件制作者出乎意料地不再热衷大量且肆无忌惮地进行垃圾邮件攻击。随后，随着需要对抗的垃圾邮件减少，反垃圾邮件系统有幸得以投入更多的计算机处理资源来分析较少的邮件，应对基于邮件的威胁。但是，正如时尚界的谚语所言“旧物换新颜”。垃圾邮件数量已开始回升。

今年，2016 年，垃圾邮件总量已悄然爬升至很长时间以来的一个最高水平。我在此向大家展示“图 A”：根据复合块列表 (CBL) 的十年垃圾邮件数量曲线。根据 CBL，上一次垃圾邮件数量达到这种水平是在 2010 年中期。



根据复合块列表 (CBL) 显示自 2009 年以来的总垃圾邮件数量的图表

接下来我要向大家展示“图 B”：SpamCop 生成的内部图表。该图表说明了过去一年 SpamCop 块列表 (SCBL) 的总规模。请注意，在 2016 年之前，SCBL 大小基本上徘徊在 200,000 个 IP 地址左右，而最近其平均值更接近 400,000 个 IP 地址，其中八月份达到最高峰，超过了 450,000 个 IP 地址。



根据 SpamCop 块列表 (SCBL) 的垃圾邮件规模图表。行计数 == IP 计数。

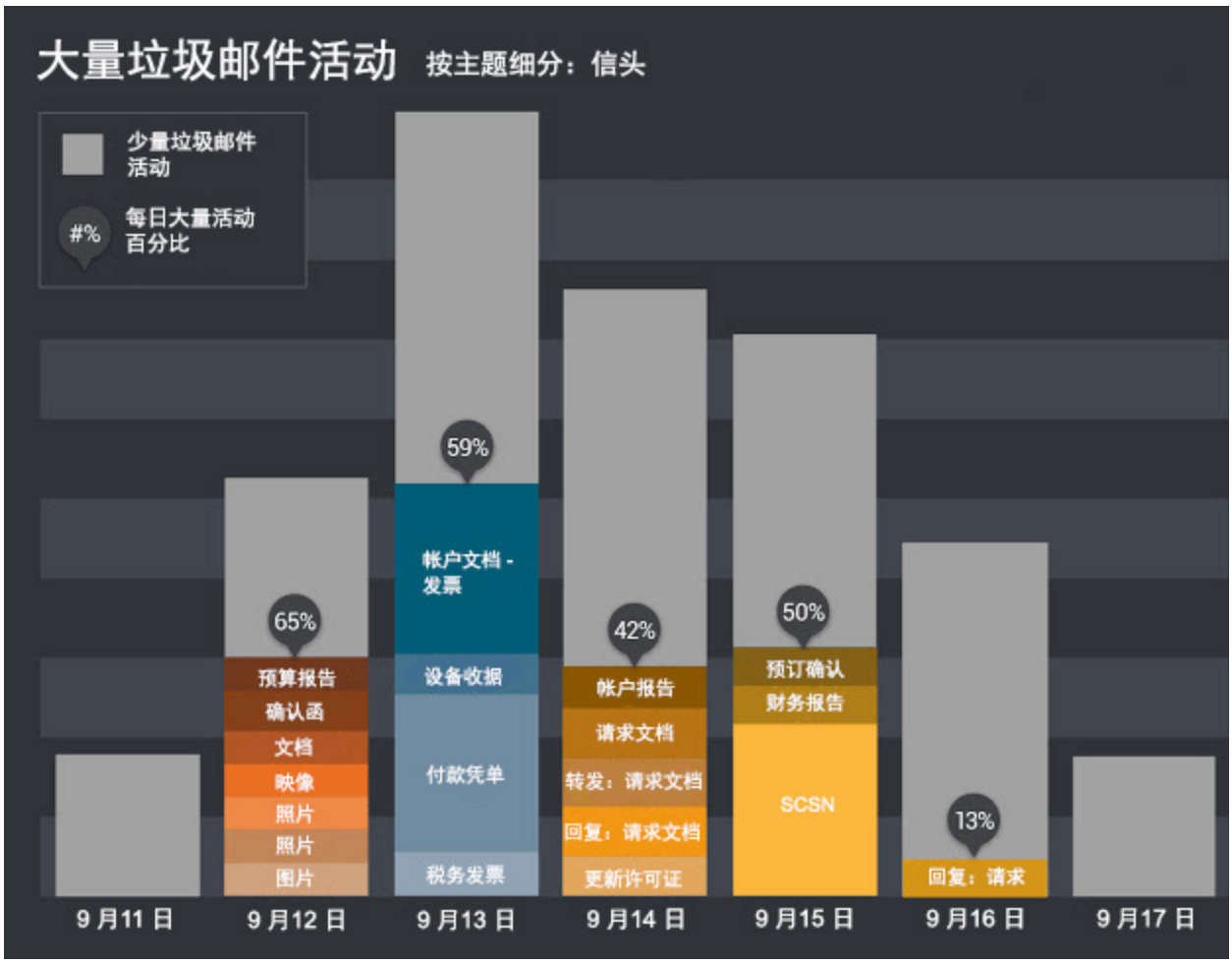
打开闸门

大批量垃圾邮件活动通常由垃圾邮件程序发送，此外，由于垃圾邮件活动在一定程度上采取的非靶向/猎射方法，反垃圾邮件系统会非常迅速地捕获它们。既然如此，垃圾邮件制作者加大垃圾邮件数量可能获得什么好处？

我们无法预测未来，无法在垃圾邮件攻击发起之前将其制止。因此，在任何经合理精心设计的垃圾邮件活动中，在垃圾邮件活动开始之后和防御者部署反垃圾邮件防护产品以应对此垃圾邮件活动之前，始终存在非常短暂的一个时间窗口。在大多数反垃圾邮件系统中，垃圾邮件制造者面临的这种“时机”可能接近几秒钟或几分钟。

对于这些垃圾邮件制作者，他们不是要让其邮件列表更具针对性，或部署雪鞋式技术降低数量并保持潜伏躲避检测，而是要跑赢这个时机。他们会尽可能多地传输网络电子邮件，而且可能会在短时间内成功地将恶意邮件发送至受害者收件箱。

对于这方面的证据，我们可以信手拈来。分析过去一周的邮件遥感勘测数据，就可以很容易地发现这些大批量垃圾邮件活动的影响。



显示 9 月 11 日至 18 日的大批量垃圾邮件活动的图表

例如，9 月 12 日，大量垃圾邮件活动几乎占当天所发送全部垃圾邮件的三分之二。另请注意周末期间活动中的间隙，垃圾邮件制作者似乎在周末休息。对于职业犯罪分子，传输垃圾邮件是其“日常工作”。

原因分析

垃圾邮件的这种全球性增长背后的恶势力是什么？思科 Talos 认为这种增长在很大程度是 Necurs 僵尸网络导致的。

发送 Necurs 垃圾邮件的许多主机 IP 都已感染两年多。为帮助充分掩蔽此僵尸网络，Necurs 仅从其控制的部分“已感染”主机发送垃圾邮件。受感染主机可能使用两至三天，然后有时候会间隔两至三个星期都不再使用。这使得响应垃圾邮件攻击的安全工作人员工作明显更加复杂化，因为尽管安全工作人员可能认为自己已经随即发现并清理发起攻击的主机，但是实

际上 Necurs 背后的犯罪分子不过是在消磨时间，他们会突然再次重新开始垃圾邮件攻击。在 Talos，我们反复看到很多 Necurs 附属 IP 经常出现这种攻击模式。

一些读者可能还记得，思科 Talos 的 Nick Biasini 曾在博文中介绍了俄国有关 Lurk 木马的抓捕事件。2016 年 6 月初俄国实施这次抓捕之后，许多活跃的威胁陷入沉寂。Necurs 垃圾邮件僵尸网络就是其中之一（见上文 SpamCop 图表）。然而，仅在几周后，就在反垃圾邮件制作者打开香槟庆祝时，Necurs 杀了个回马枪。Necurs 不仅杀了个回马枪，而且还从主要发送关于交友约会和股票哄抬股价的俄语垃圾邮件，转变为发送恶意附件垃圾邮件。这是我们首次看到 Necurs 发送附件。这些恶意附件传播 Dridex（一种臭名昭著的银行恶意软件变体）或 Locky（一种多产的勒索软件变体）。

结论

电子邮件威胁，正如任何其他事物一样，也会不断发展。随着我们的威胁检测和阻止技术的发展，攻击者也在想方设法规避检测技术。很遗憾，没有抵御垃圾邮件活动的绝招。我们鼓励各组织建设多层防御，最大限度地增加检测和阻止此类攻击的机会。当然，每当涉及勒索软件时，离线备份对于组织的生存至关重要。组织需定期审查和测试恢复计划，确保不存在任何错误而且没有忽视任何项目。最后，与用户保持联系，确保其了解不得信任任何奇怪附件！

发布者：JAESON SCHULTZ；发布时间：下午 1:00

标签：附件、僵尸网络、DRIDEX、LOCKY、NECURS、SCBL、垃圾邮件、SPAMCOP