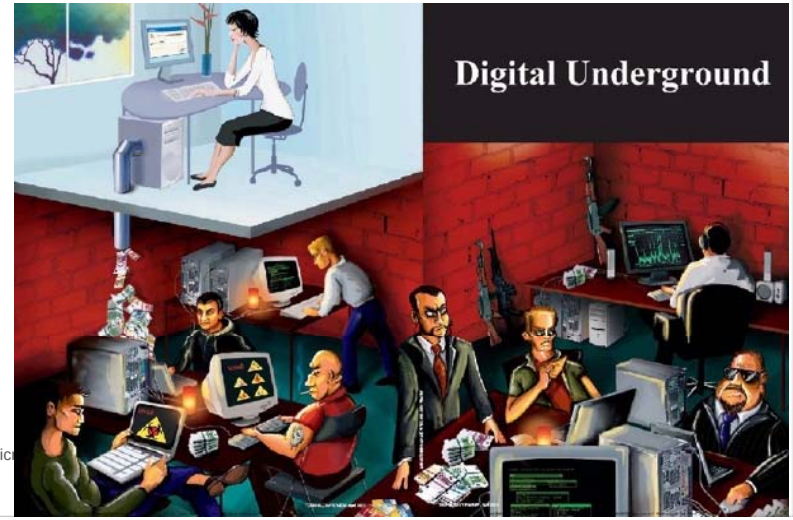
TREND MICRO™ Securing Your Web World

2010主要病毒情况回顾

Peter Zang • Trend Micro

2010年安全趋势

- 没有全球性的病毒爆发，但区域性的病毒攻击会继续持续
- 数字罪犯的最终目标仍旧是为了获得金钱
- 僵尸网络不会停止
- 新的恶意攻击可能会出现在虚拟化环境和云环境
- 病毒会在更短的时间内产生新的变种
- 公司及社交网络都会有数据泄露的危险
- Windows 7会成为攻击的对象
- 即使更换浏览器以及操作系统，都无法降低安全风险

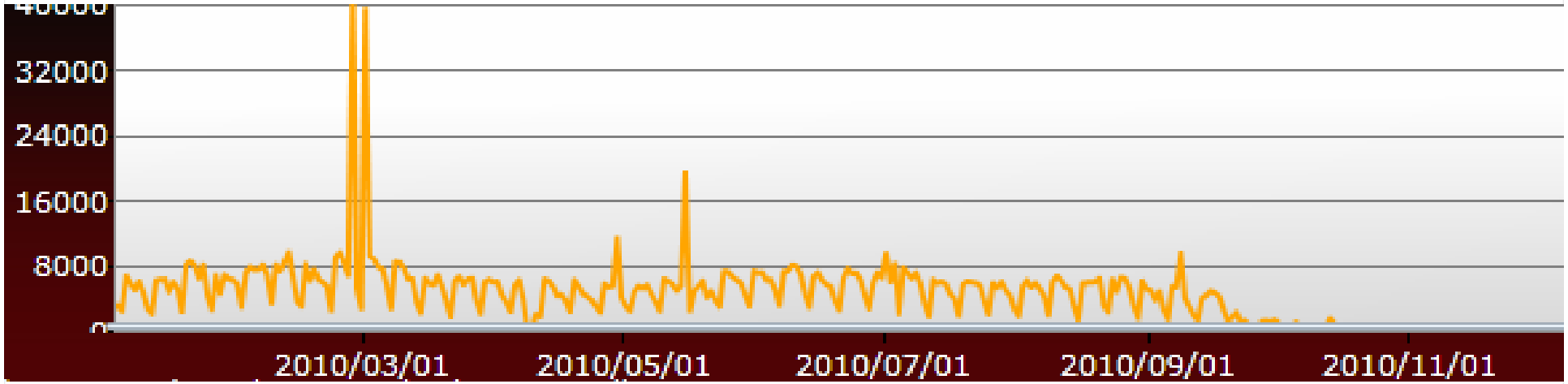


DOWNAD: 病毒区域化趋势下的全球挑战

- DOWNAD病毒（又称Conficker）是09年至10年感染力最强的病毒
- 根据监测，中国大概有180余万独立IP地址感染了该病毒，全球约有700余万独立IP地址受到感染
- DOWNAD家族的病毒通过多种方式进行传播。包括，漏洞，弱密码，共享等等。

DOWNAD家族2010年感染数量

- 2010年前三季度依然肆虐
- 第四季度起极少发作



KOOBFACE+FAKEAV
Web2.0时代的病毒传播方式

- 2008年8月： 首例KOOBFACE
- 2009年： KOOBFACE大肆在英语国家传播。
- 2010年： KOOBFACE演变
  - 利用偷来的账号散布假防毒软件（FAKEAV）等恶意链接
  - 以带有假防毒软件的变种木马感染遭入侵网站的使用者
- 2010年： KOOBFACE+FAKEAV出现在中国

病毒武器？STUXNET

- 什么是STUXNET?
  - 首个针对工业控制系统的蠕虫病毒，利用西门子公司控制系统（SIMATIC WinCC/Step7）存在的漏洞感染数据采集与监控系统（SCADA），能向可编程逻辑控制器（PLCs）写入代码
- 攻击方式：系统漏洞
  - MS10-046、MS10-061、MS08-067等7个最新漏洞
    - 5个针对Windows系统
    - 2个针对西门子SIMATIC WinCC系统

STUXNET在全球的分布

TREND MICRO

文件夹病毒: 社会工程学的典范

- 什么是文件夹病毒：
  - 是一类恶意病毒，将所有根目录下和桌面上的文件夹全部隐藏，并将自己的副本命名为文件夹的名字
- 病毒特点：
  - 病毒图标为文件夹图标
  - 在硬盘上产生大量病毒副本
  - 副本清理后，不易恢复隐藏文件夹

Q&A

谢谢！

TREND MICRO