TREND MICRO
Securing Your Web World

近期病毒流行趋势

Peter Zang • Trend Micro

流行病毒传播途径

- 漏洞
  - 利用系统漏洞传播的DOWNAD家族
- Web2.0
  - 利用社交网络传播的KOOBFACE家族
- 社会工程学
  - 利用移动存储设备传播的文件夹图标病毒

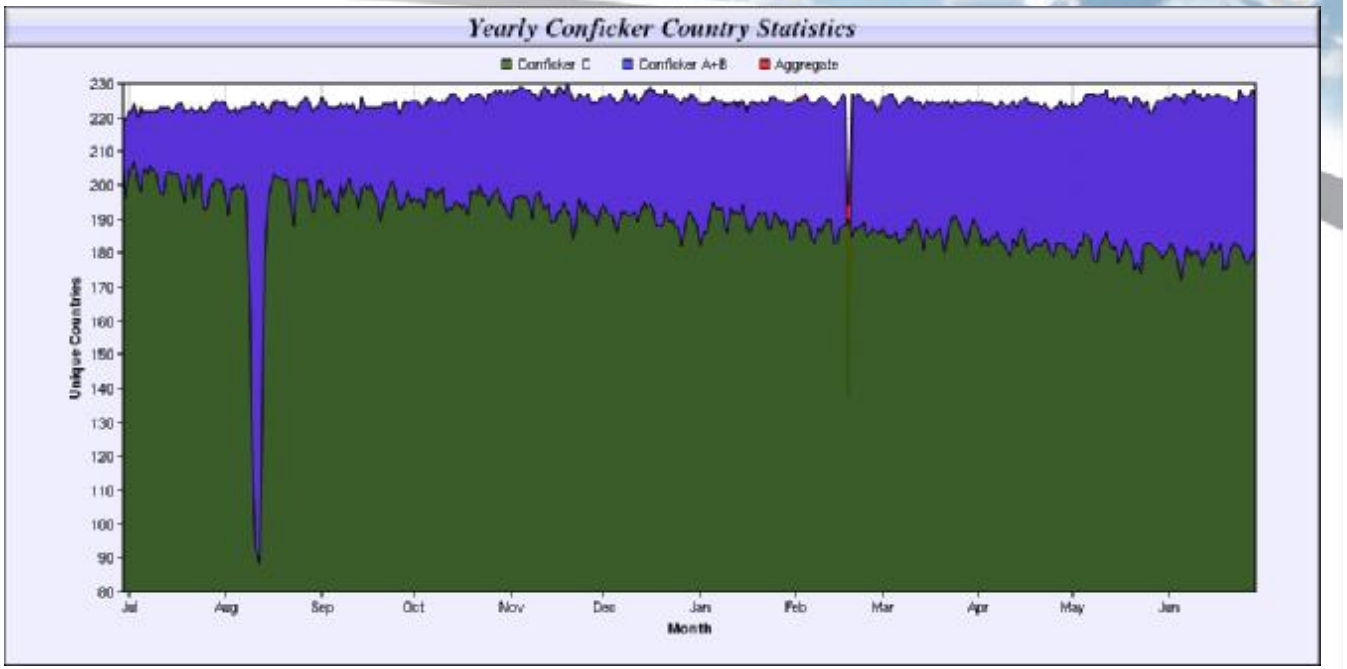
TREND MICRO

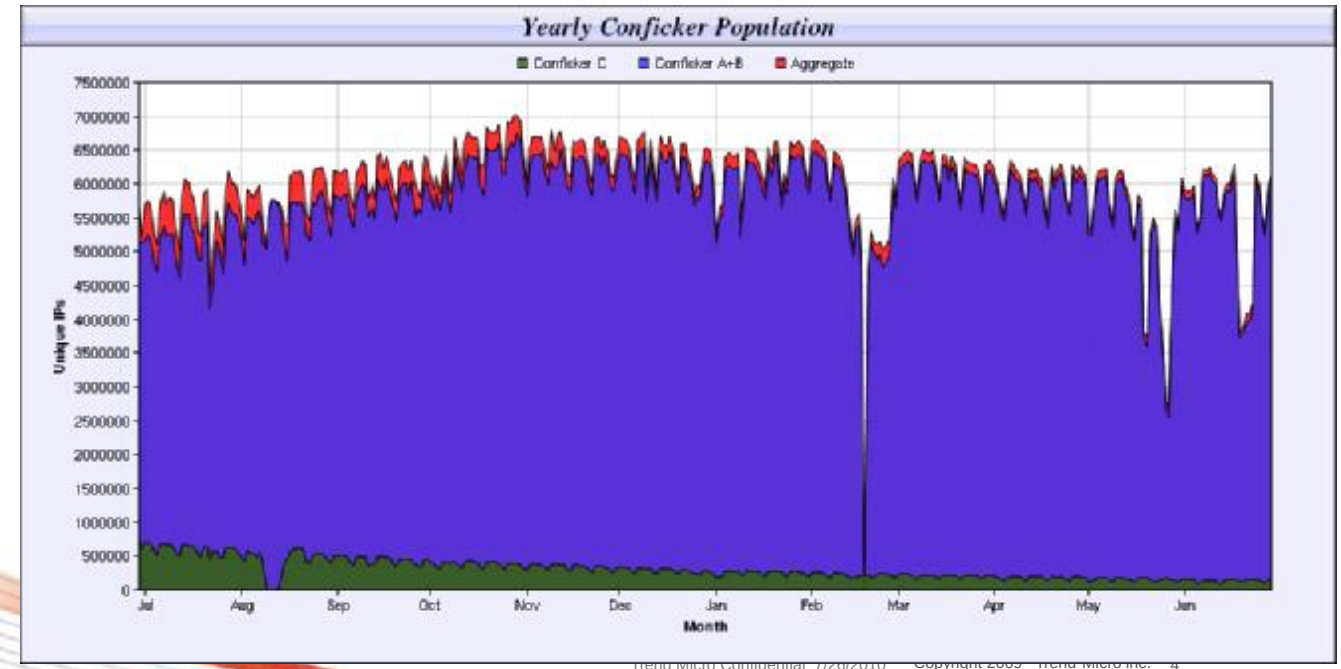
DOWNAD: 病毒区域化趋势下的全球挑战

- DOWNAD病毒（又称Conficker）是09年全年当中感染力最强的病毒，也是09年全球传播最广泛的病毒
- 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。

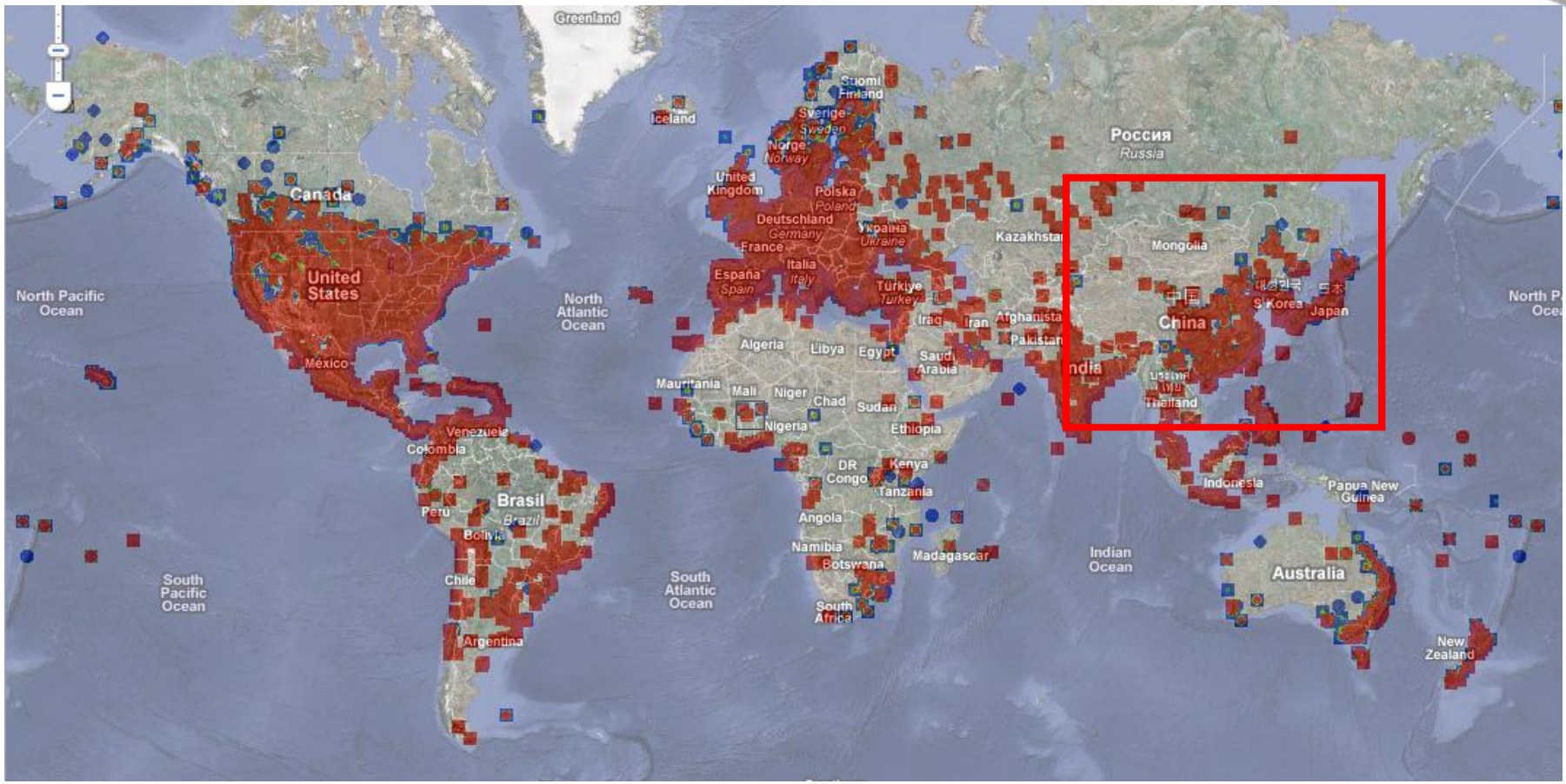
TREND MICRO

受影响国家数量





受影响IP数量

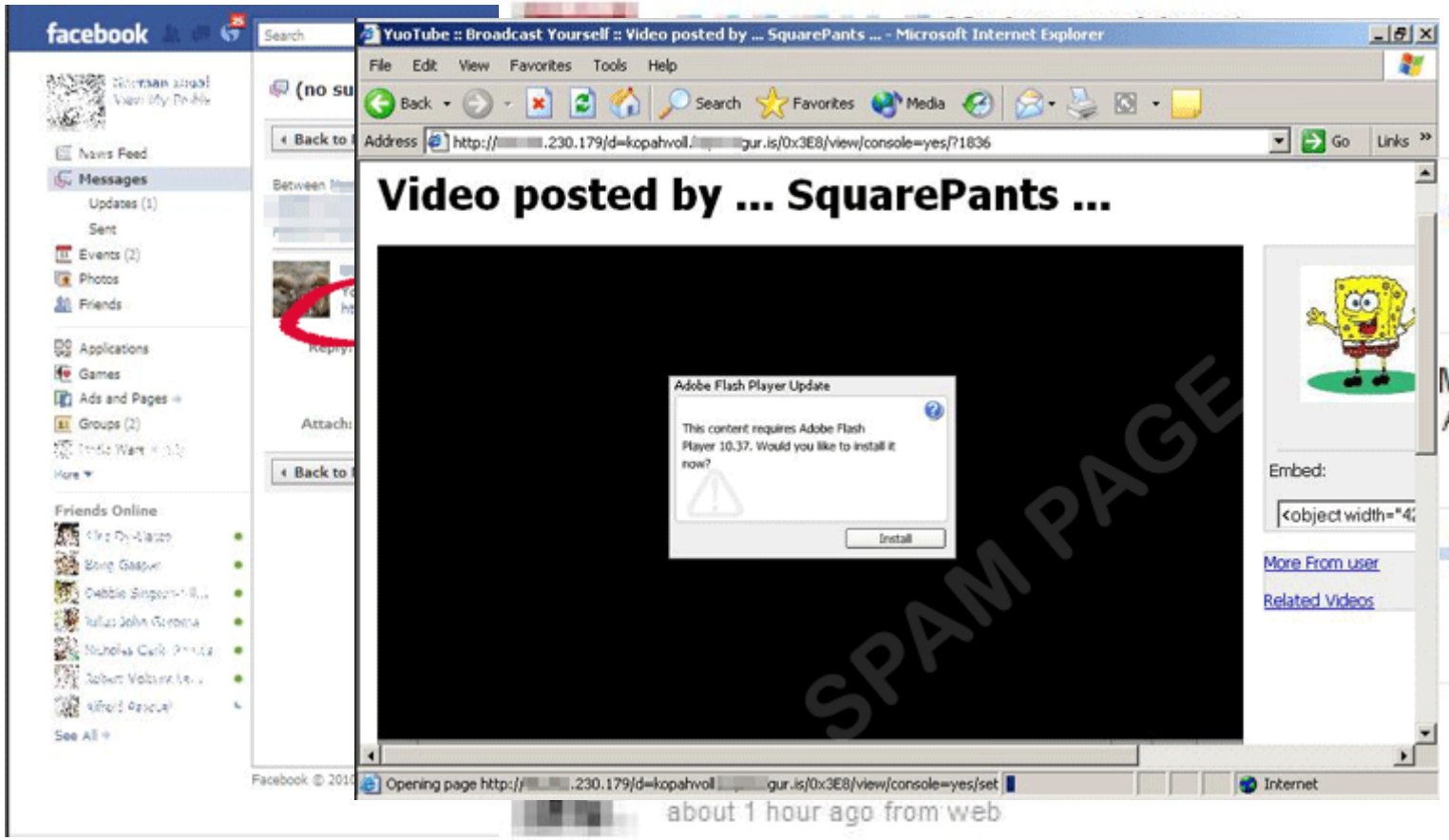


KOOBFACE: Web2.0时代的病毒传播方式

- 有社交网络祸害之称的KOOBFACE为典型的Botnet僵尸网络。
- KOOBFACE 首例发现于 2008 年 8 月，在2009年3月中旬到8月中旬间，Trend Micro趋势科技威胁专家已确定约有51000的受破坏的计算机目前正为此僵尸网络所利用，并纪录到约46个KOOBFACE的指挥控制中心的网域。
- KOOBFACE其原始的设计只是盗用账号，演变到利用偷来的账号散布假防毒软件（FAKEAV）等恶意链接，或以带有假防毒软件的变种木马感染任何只是恰巧进入遭入侵 网站的使用者，受害者只要点击恶意网页的任何一处链接，即会下载恶意软件。

TREND MICRO

KOOBFACE通过SNS传播



Facebook Spam

Rogue Flash Player Twitter Spam

TREND MICRO

文件夹病毒: 社会工程学的典范

- 文件夹类病毒是一类恶意病毒，它会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。
- 由于病毒的图标就是文件夹图标，如果没有显示扩展名的话很容易中招。
- 病毒会在硬盘上产生大量的病毒副本，即使副本被清理掉了，恢复隐藏的文件夹对用户也是一件不容易的事情。

社会工程学

- “社会工程”这个词，作为一个心理操纵行为，由黑客出身的顾问Kevin Mitnick提出并推广。

- 社会工程是操纵人的行为或泄漏机密信息的一种行径。不同于一般的技术入侵手段，社会工程更多利用欺骗的手段。该手段类似于骗局或简单的欺诈，通常被用于描述以收集信息或获取计算机系统权限为目的的欺骗行为。在大多数情况下，攻击者与受害者不会进行面对面的交锋。

中毒用户直观感受

双击文件夹

打开文件夹

真的只是打开了一个文件夹吗？

事情真的只是这么简单？

实际情况

- 病毒复制自身副本
- 增加病毒副本自启动项
- 关闭显示隐藏文件选项
- 打开文件夹  用户可感知过程
- 遍历隐藏文件夹
- 将病毒副本以被隐藏的文件夹名称存放至相同位置
- 释放autorun.inf及病毒副本
- 感染移动存储器

TREND MICRO

为何如此流行？

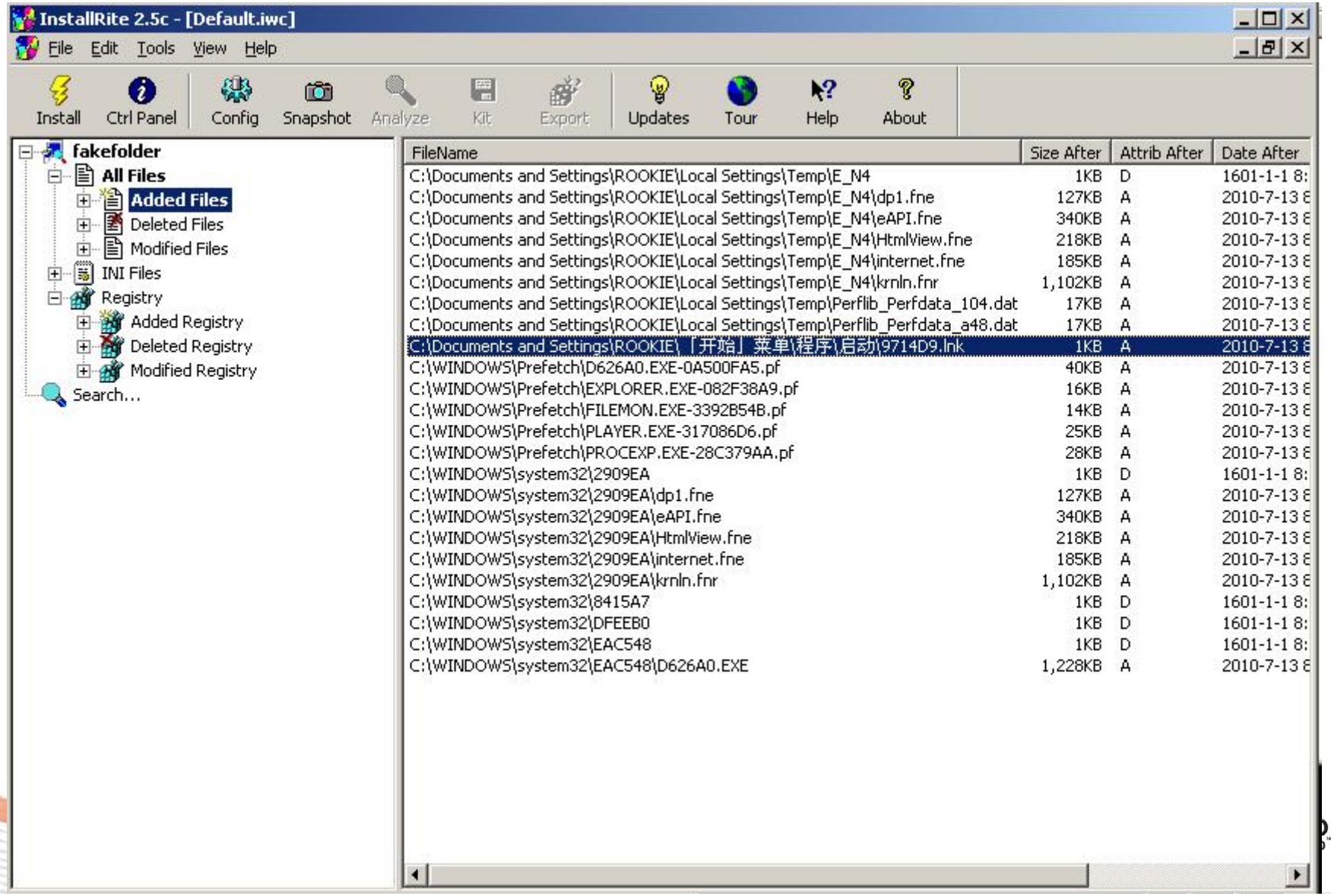
计算机使用者	计算机
通过可见文件名辨识	通过完整文件名辨识
图标为重要辨识依据之一	图标不作为辨识依据
认为双击执行的操作为打开	双击执行的操作可自定义
习惯性操作	无习惯性，忠实执行每一条命令
知识水平及了解程度影响判断	忠实执行命令，无主观影响

矛与盾

- 社会工程学是病毒之矛
- 良好的计算机使用习惯是用户之盾
  - 显示隐藏及系统文件
  - 显示已知文件类型后缀
  - 使用资源管理器树形窗口打开磁盘及文件夹
  - 等等……

TREND MICRO

Look Inside



Q&A

谢谢！

TREND MICRO