【网络攻防-大作业】

僵尸网络(Botnet)和高级持续性威胁(APT)是网络安全领域重要研究方向,近年来,防御者通过分析 Botnet/APT 攻击过程使用的恶意软件、C&C 服务器,可以有效实现对攻击源头的溯源。

本课大作业内容如下:

大作业由三个小作业组成,三个小作业均为必选。

小作业 1:**Botnet 控制者溯源**

Botnet 控制者常常远程连接到 C&C 服务器进行操作,研制一个 Botnet 控制者溯源辅助分析工具。该工具运行在开启 Windows 远程桌面服务的(端口号 3389)服务器上,当远程客户端(可能是 Botnet 控制者)连接时,该工具可以提取出远程客户端操作系统相关信息,包括键盘布局、系统语言、IP 地址等至少 4 种指纹信息;

小作业 2:APT 攻击者溯源

APT 攻击发起者常常在制作的 Malware 中不小心留下身份信息,研制一个 APT 攻击者溯源辅助分析工具,实现对可执行文件和办公文档中"身份信息"的自动提取,要求可执行文件至少支持 PE 格式、办公文档至少支持两种自选格式,且其中一种为 Word 或 PDF 格式;

小作业 3: Botnet 新型 C&C 技术

未来 Botnet 可能会不断采用新技术来对抗防御措施,提出一种尚无公开报道(或发表)的 C&C 思路,并验证可行性,形成一个 Demo 或技术文档。已公开的 C&C 思路,包括但不限于 IRC、HTTP/HTTPS、P2P、DNS TXT、Gmail/Yahoo、Google App Engine、Google Docs、Internet Clipboard、Domain Flux、Fast-Flux、Shorten URL、Twitter、Pastbin、Skype、Email、Search Engine 等。提示:最近三年出现的新服务新应用,很多可以被用作 C&C,还可以通

过多种方法组合应用，实现 C&C 新模式。

注：以上均可充分利用开源代码与工具。

关于分组：

（1）每个分组的人数为 11—15 人之间，特殊情况可增加 1-2 人，需提交原因给助教。

（2）每个分组选出一名组长和三名小组长（对应三个作业内容），组长需兼任某一作业的小组长。所以，组长与小组长数量之和等于三。

（3）提交大作业时，由组长团队商议指定每个人的贡献度（用百分比形式，以作业为单位）。

举例，学生 A 为组长并兼任作业 1 的小组长，学生 B 为作业 3 的小组长，作业 3 的成员为 C 和 D，则由 A 和 B 共同确定学生 B、C、D 在作业三的贡献度的百分比。

大作业提交形式：

提交小作业 1-2 所研制工具的源代码及相关技术说明文档，小作业 3 的演示 Demo 或技术文档，同时形成课堂交流 PPT，用于 2017.5.9 课堂上研讨，PPT 建议由各个小组长分别介绍讲解。

大作业提交方法：

请于 2017.5.1 之前通过邮件提交，由组长将大作业及每人贡献度发送邮件到 liuchaoge@iie.ac.cn，并抄送到 cuixiang@iie.ac.cn。体积过大不能发送邮件时，请与助教刘潮歌老师协商提交方式。