恶意软件发现与分析

第1章 恶意软件概述

主要内容

- 1.1 恶意软件分析概述
- 1.2 课程简介（代表课程团队）

1.1 恶意代码概述

恶意代码分析目标

恶意软件是什么？

- 恶意软件的定义
  - 恶意软件（Malware）是对非用户期望运行的、怀有恶意目的或完成恶意功能的软件的统称。恶意软件种类繁多，如木马、病毒、蠕虫、DDoS、劫持、僵尸、后门/陷门、恶意编译、间谍软件、广告软件、勒索软件、跟踪软件等
- 早期（狭义）
  - 病毒、蠕虫
- 当今（广义）
  - 多种多样、“蓬勃发展”，包括：APT

恶意软件的发展

- 一般来说3个阶段
  - 第一阶段，单机传播。在上世纪80年代，计算机应用以单机为主，计算机之间的数据交换主要借助于磁盘，因此，当时的恶意软件主要是磁盘病毒、文件宏病毒；
  - 第二阶段，网络传播。随着网络技术的发展和应用，计算机之间实现了直接互联，邮件等应用也越来越普遍，随之而来的是Melissa、Loveetter、Nimda和Code Red等邮件病毒和蠕虫；
  - 第三阶段，协同攻击。传统的病毒、木马实施破坏仍以单一的节点单独实施，而僵尸网络的出现，则实现了被感染节点之间的协同。典型代表P2P僵尸网络

事件响应

- 案例
  - 一个诊所有10个办公室，在他们的服务器上发现恶意代码
  - 请人来清理并重装计算机
- 完事—事情结束了吗？

事件响应

- 发现恶意代码后，还需掌握
  - 攻击者是否在系统中植入了 rootkit 或者木马？
  - 攻击者真的消失了吗？
  - 攻击者窃取或添加了什么？
  - 这次攻击是怎么发生的？
    - 根源分析

清理花费LinkedIn近1百万美元，另外2-3百万美元用于升级

Breach clean-up cost LinkedIn nearly $1 million, another $2-3 million in upgrades

Summary: *LinkedIn executives reveal on quarterly earnings call just what the June theft of 6.5 million passwords cost the company in forensic work and on-going security updates.*

By John Fontana for Identity Matters | August 3, 2012 -- 17:10 GMT (10:10 PDT)

Follow @johnfontana

Comments 0 | Vote 1 | Like 4 | Tweet 51 | Share | more +

LinkedIn spent nearly $1 million investigating and unraveling the theft of 6.5 million passwords in June and plans to spend up to $3 million more updating security on its social networking site.

恶意代码分析

- 通过剖析代码来理解
  - 它是如何工作的
  - 如何辨别它
  - 如何衡量并消除它所带来的危害
- 事件响应中的重要组成部分

恶意代码分析目标

- 应对网络入侵所需信息
  - 到底发生了什么
  - 找出所有被感染的机器和文件
  - 如何衡量并消除损害
  - 为入侵检测系统找到特征码

特征码

- 基于主机的特征码
  - 识别**受害者电脑上**被恶意代码感染的**文件或注册表**键值
  - 关注恶意代码做了什么，而不是恶意代码本身
    - 与反病毒软件所使用的病毒特征码不同
- 网络特征码
  - 通过分析网络流量监测恶意代码
  - 在恶意代码分析帮助下更有效

恶意代码分析技术

静态与动态分析

- 静态分析
  - 在不运行恶意代码的情况下对它进行分析
  - 工具： VirusTotal、strings、反编译工具如IDA Pro
- 动态分析
  - 运行恶意代码并监控其效果
  - 使用虚拟机快照
  - 工具： RegShot、Process Monitor、Process Hacker、CaptureBAT
  - 内存分析： 峰值及波动

基础技术

- 静态分析基础技术
  - 检查恶意代码但不用查看指令
  - 工具： VirusTotal、 strings
  - 快速、简单但对复杂恶意代码很大程度上是无效的，而且可能错过一些重要的行为
- 动态分析基础技术
  - 简单，但需要安全的测试环境
  - 并不是对所有恶意代码都有效

高级技术

- 静态分析高级技术
  - 逆向工程，使用反汇编软件
  - 复杂，需要理解的汇编代码
- 动态分析高级技术
  - 在调试器中运行代码
  - 检测恶意执行程序运行时的内部状态

恶意代码分析通用规则

恶意代码分析通用规则

- 不用过于陷入细节
  - 不需要100%的理解所有代码
  - 关注关键特征
- 尝试使用一些工具
  - 如果一个工具失效，试试另一个
  - 别卡在一个难题上，尝试转移到其他问题
- 恶意代码编写者在不断提升抗分析技术

恶意软件相关的学术研究

- 恶意软件及漏洞相关的学术和技术会议
  - 学术
    - S&P
    - CCS
    - USEnix Security…
  - 技术
    - Blackhat
    - …

1.2 课程简介

（代表课程团队）

为什么要开设本课程

- 网络空间安全的核心内容；
- 网络攻防技术的基础之一；
- 和学院的多门其他课程形成联动
  - 《软件安全与脆弱性分析》
  - 《软件安全漏洞分析与发现》
  - 《网络攻防》
  - 《网络安全风险评估与应急响应》

课程大纲

（注意：提倡积极主动的学习态度）

- **第一章 恶意软件概述(2课时、刘剑)**
  - 介绍恶意软件的基本概念、工作机制、历史、技术分类、发展趋势等相关问题。
- **第二章 恶意软件发现技术（4课时、刘剑）**
  - 介绍文件扫描、主机行为检测、通信行为检测、相似性检测等常见的恶意软件发现技术。
- **第三章 软件分析技术基础（4课时、刘剑）**
  - 介绍PEView、Dependency Walker、Process Explorer、Regshot等常见的静态分析和动态分析基础技术。
- **第四章 静态分析高级技术（6课时、刘剑）**
  - 首先介绍x86反汇编、IDA Pro等基础静态分析知识，在此基础之上介绍分析Windows恶意程序的方法。
- **第五章 动态分析高级技术（4课时、刘剑）**
  - 介绍动态调试、OllyDbg等动态分析基础知识，在此基础之上介绍如何使用WinDbg调试Windows内核。
- **第六章 恶意软件功能（8课时、赵双\刘剑）**
  - 介绍Windows平台下的恶意软件的主要功能特点，包括恶意攻击行为、隐蔽代码启动、数据加密、恶意代码网络特征等。

Windows平台恶意软件

课程大纲

- **第七章 恶意软件对抗技术（4课时、赵双\刘剑）**
  - 介绍反汇编、反调试、反虚拟机技术等恶意软件对抗及分析技术。
- **第八章 Linux恶意软件（2课时、赵双\刘剑）**
  - 介绍Linux平台下可执行文件（ELF）结构、Linux恶意脚本、ELF恶意软件等内容。
- **第九章 智能终端恶意软件（4课时、赵双\刘剑）**
  - 介绍智能终端恶意软件的基本概念和技术发展，并详细分析Android平台的恶意软件攻击方法和实现技术。
- **第十章 其他恶意软件（2课时、赵双\刘剑）**
  - 介绍流氓软件、勒索软件、僵尸网络、网页木马、Rootkit等近年新兴的恶意软件
- 小结：
  - 1-7章（除第2章）和参考书1中1-18章基本对应；8-10章主要是教学团队自己增加的前沿内容；
  - 3次课后作业（homework）：实验任务，提交代码到课程网站；
  - 1次期末开卷考试；

Windows平台恶意软件

Linux平台恶意软件

Android等智能终端

授课团队

- 刘剑（首席教授）：liujian6@iie.ac.cn
  - 主要研究软件与系统安全、移动安全、Web安全、程序分析、安全测试等
  - 在IEEE TSE、ACM TODAES、ICSE、FSE等国际顶期刊/会议发表多篇学术论文
- 赵双（主讲教师）：zhaoshuang@iie.ac.cn
  - 重量级畅销图书《0day安全:软件漏洞分析技术》主要作者之一
  - 多项国家级项目的技术骨干
  - XCon,HitCon,OWASP China等国内外安全峰会Speaker

授课团队

- 陈宏程
  - 邮件：chenhongcheng@iie.ac.cn
- 国科大课程网站
  - 课件
  - 课程课件
- 课程微信群
  - 课程重要通知
  - 师生互动

参考书

- 课堂
  - **《恶意代码分析实战》，电子工业出版社，Michael Sikorski等著，诸葛建伟等译**
- 课外
  - 《恶意代码与计算机病毒 — 原理、技术和实践》，清华大学出版社，刘功申、孟魁
  - 《恶意软件分析诀窍与工具箱》，清华大学出版社，（美）Michael.Hale.Ligh等著

考核与评分（待定）

- 课堂表现：10分
- 课程作业：40分（10分+15分+15分）
- 课堂开卷考试：50分

- 课程项目：利用所学知识完成一个程序分析工具，具有一定的实用价值

关于课程作业

- 课程作业3次
  - 根据课程讲解的进度，在重要节点设置（暂定）
    - 第1次：动静态分析技术
    - 第2次：高级分析技术+恶意软件功能
    - 第3次：恶意软件对抗
  - 内容：主要是恶意软件分析报告，包括基础题（课本知识）+附加题（有一定挑战）
  - 提供实验环境
- 注意事项
  - 鼓励有建设性的交流和学习；
  - **坚决杜绝“简单粗暴”的抄袭（你的作业不要给别人，因为我们无法判定谁抄袭谁），有很多特征区别你和别人的不同点，例如作业时间、内存地址等；**

关于课件

- 课件的分享
  - **课件版权归国科大和课程授课团队所有，严禁未经许可通过网络或者其他途径发布。**