CAN304 W9

Overview of malware

Malicious software：任何故意设计用于对计算机、服务器、客户端或计算机网络造成损坏的软件。

Compromise CIA，Annoy or disrupt the victim。

Malware types

一种流行的恶意软件分类方法：首先了解它如何传播 (spreads or propagates) 以达到所需的目标，然后了解它在到达目标后执行的操作或有效载荷 (actions or payloads)。

还按以下分类：

- 需要主机程序的恶意软件（寄生代码，parasitic code）
- 独立的 (independent and self-contained) 恶意软件
- 无法复制的恶意软件
- 可以复制 (replicate) 的恶意软件

Propagation mechanisms

- 病毒感染现有内容，随后传播到其他系统
- 蠕虫 (worms) 或下载驱动 (drive-by-downloads) 利用软件漏洞，允许恶意软件复制
- 说服用户绕过安全机制安装 Trojans 木马或响应网络钓鱼攻击 (phishing attacks) 的社会工程攻击 (Social engineering attacks)

Payload actions

- 系统或数据文件损坏 (corruption)
- 盗窃服务 (Theft of service) 或使系统成为僵尸网络 (botnet) 一部分的攻击僵尸代理 (zombie agent)
- 从系统中窃取信息/键盘记录
- 将其存在隐藏在系统上以使其隐身 (stealthy)

Attack kits

攻击工具包通常被称为“犯罪软件 (crimeware)”，包括各种传播机制和有效负载模块，即使是新手也可以部署。例如：Zeus，Blackhole，Sakura，Phoenix。

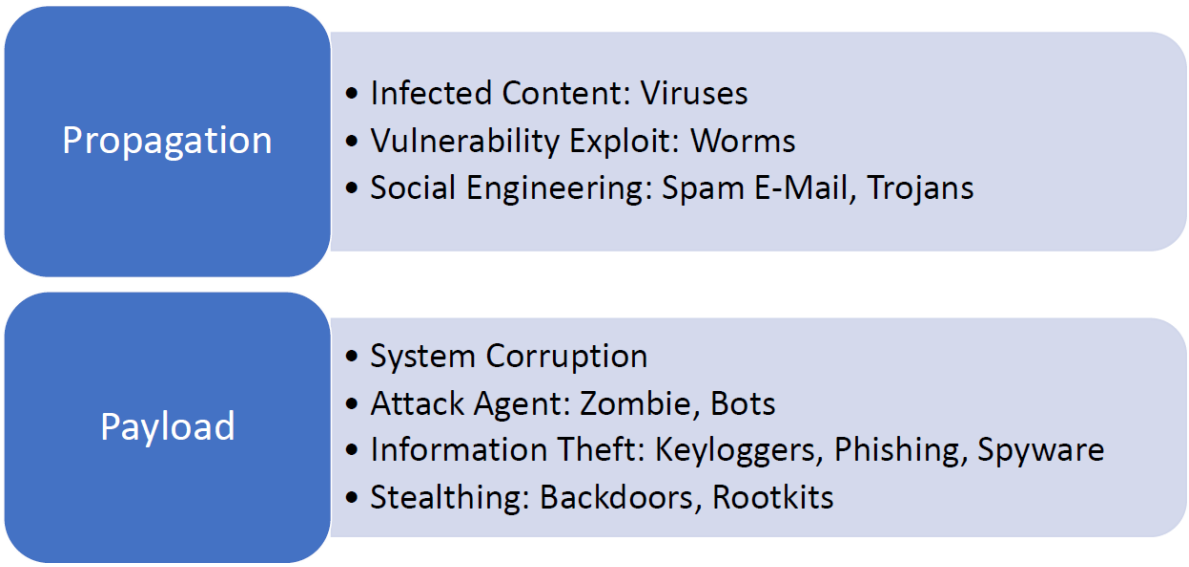
Attacker source

早期攻击者：个人通常有动力向同龄人展示他们的技术能力。

现在：更有组织和更危险的攻击源。例如：Politically motivated attackers，Criminals，Organized crime，Organizations that sell their services to companies and nations，National government agencies。

Common types of malware

Common types of malware



Propagation

Infected Content: Viruses

Viruses

- 感染程序的软件：修改程序以包含病毒的副本，复制并继续感染其他内容
- 当附加到可执行程序时，病毒可以执行该程序允许执行的任何操作

Virus components

- Infection mechanism：病毒传播的手段，也称为感染媒介 (infection vector)
- Trigger：确定何时激活或交付 payload 的事件或条件，有时被称为逻辑炸弹 (logic bomb)
- Payload：病毒做什么（除了传播），可能涉及损伤或良性但明显的活动

Virus phases

- Dormant phase
  - 病毒处于空闲状态 (idle)；最终将被某些事件激活；并非所有病毒都有此阶段
- Propagation phase
  - 病毒将自身的副本放入磁盘上的其他程序或某些系统区域；可能与传播版本不同；每个受感染的程序现在将包含病毒的克隆，该克隆本身将进入传播阶段
- Triggering phase
  - 病毒被激活以执行其预期的功能；可能由各种系统事件引起
- Execution phase
  - 执行功能；可能无害或有害

如何检测病毒？ - 通过判断文件大小，File-size based detection；可以通过压缩病毒来避免被检测到。

Vulnerability Exploit: Worms

Worms

一个独立的恶意软件计算机程序，可以自我复制以传播到其他计算机。利用软件漏洞。可以使用网络连接在系统之间传播。通过共享媒体（USB 驱动器、CD、DVD 数据磁盘）进行传播。电子邮件蠕虫在附件中包含的宏或脚本代码中传播。激活后，蠕虫可能会复制并再次传播。

Warm propagation

传播阶段通常执行以下功能：

搜索对要感染的其他系统的适当访问机制，然后使用找到的访问机制将自身的副本传输到远程系统，并运行该副本。

Worm and Virus

两者类似，术语通常可互换使用。病毒试图感染其他程序，蠕虫寻求从一台机器移动到另一台机器。

Drive-by-downloads

当用户查看攻击者控制的网页时，利用浏览器漏洞在系统上下载并安装恶意软件。在大多数情况下不会主动传播，当用户访问恶意网页时传播。

Social Engineering: Spam E-Mail, Trojans

Social engineering

“欺骗 (Tricking)”用户以协助破坏自己的系统：

- Spam / phishing e-mails
    - 未经请求的批量电子邮件；恶意软件的重要载体；用于网络钓鱼攻击
- Trojan horse
    - 看似有用的程序，包含执行有害操作的代码
- Mobile phone Trojans
    - 目标是智能手机

Payload

System Corruption

Data destruction：

- Chernobyl virus：感染可执行文件，并在达到触发日期时损坏整个文件系统
- Klez：通过电子邮件传播的计算机蠕虫，在触发日期导致硬盘驱动器上的文件变为空
- Ransomware：加密用户的数据并要求付款，以便访问恢复信息所需的密钥

Logic bomb：恶意软件中嵌入的代码，设置为在满足某些条件时“爆炸”。

Triggers：

- 系统上存在或不存在某些文件或设备
- 一周中的特定日期或日期
- 某些软件的特定版本或配置
- 运行应用程序的特定用户

Attack Agent: Zombie, Bots

接管另一台连接互联网的计算机，并使用该计算机发起或管理攻击。

Botnet - 能够以协调方式行事的机器人的集合。

用于：Distributed denial-of-service (DDoS) attacks，Spamming，Sniffing traffic，Keylogging，Spreading new malware。

Information Theft: Keyloggers, Phishing, Spyware

键盘记录器和间谍软件 (Keyloggers and Spyware)

- Keylogger：捕获击键以允许攻击者监控敏感信息，通常使用某种形式的过滤机制，仅返回接近关键字的信息（“login”，“password”）
- Spyware：颠覆受感染的机器，以允许监视系统上的各种活动；监视浏览活动的历史记录和内容；将某些网页请求重定向到虚假站点；动态修改浏览器和某些感兴趣的网站之间交换的数据

Phishing (网络钓鱼)：利用社会工程学伪装成来自受信任来源的通信，从而利用用户的信任。

- 在垃圾邮件中包含一个 URL，该 URL 链接到模仿银行、游戏或类似网站的登录页面的虚假网站
- 建议用户需要紧急操作来验证他们的帐户
- 攻击者使用捕获的凭据利用该帐户

Stealthing: Backdoors, Rootkits

Backdoor

- Also known as a trapdoor
- 程序的秘密入口点，允许攻击者获得访问权限并绕过安全访问程序
- Maintenance hook 是程序员用来调试和测试程序的后门
- 接管机器的恶意软件通常会插入 trapdoor，为了让攻击者重新进入。应小心处理受感染的机器以移除此类 trapdoor

Rootkit

- 旨在维护对计算机的非法访问的软件
- 在攻击者在系统上获得非常特权访问之后被安装，目标是确保持续的特权访问 (通过隐藏恶意软件的存在，和通过防御删除 (defending against removal))

Countermeasures

Malware countermeasure approaches

- Prevention
  - Policy
  - 确保所有系统都尽可能保持最新状态 - Reduce vulnerabilities
  - 对应用程序和数据设置适当的访问控制
  - 提供适当的用户意识和培训
- Mitigation
  - options：Detection，Identification or Removal
- Backup

General requirements for countermeasures

- Generality
- Timeliness
- Resiliency
- Minimal denial-of-service costs
- Transparency
- Global and local coverage

Generations of anti-virus:

- First generation: simple scanners
  - 需要恶意软件签名来识别恶意软件；另一种方法是长度检查 (size)
- Second generation: heuristic scanners
  - 使用启发式规则搜索可能的恶意软件实例；另一种方法是完整性检查 (使用 checksum)
- Third generation: activity traps
  - 通过恶意软件的行为而不是受感染程序中的结构来识别恶意软件
- Fourth generation: full featured protection
  - 包含多种反病毒技术结合使用的软件包

Generic decryption

使防病毒程序能够轻松检测复杂的多态病毒和其他恶意软件，同时保持快速的扫描速度。

可执行文件通过包含以下元素的GD扫描仪运行：CPU 仿真器，病毒特征扫描器，仿真控制模块

Host-based behavior-blocking software

与主机操作系统集成，实时监控程序行为以防恶意行为 - 在潜在的恶意操作有机会影响系统之前阻止它们；实时阻止软件，因此它比指纹识别或启发式等防病毒检测技术更具优势。

限制 - 因为恶意代码必须在目标机器上运行才能识别其所有行为，因此它可能在被检测和阻止之前造成危害。