# 特种木马攻击与溯源

天融信阿尔法实验室

冷风

# 你可以了解到：

1. 特种木马的一些特性

2. 攻击溯源的一些思路

# 目录


1 穿透ISA代理及硬件代理

2 绕过流量监控及地址检测

3 使用多协议进行内容穿透

4 协议加密穿透IPS/IDS

5 使用隧道穿透单机防火墙

6 对抗虚拟机检测

7 对抗启发式检测

8 目前杀软的软肋

1 我们的对手是谁

2 溯源之难

2 如何发现特种木马

3 基于二进制的分析

4 基于IP的分析

5 基于蜜罐的分析

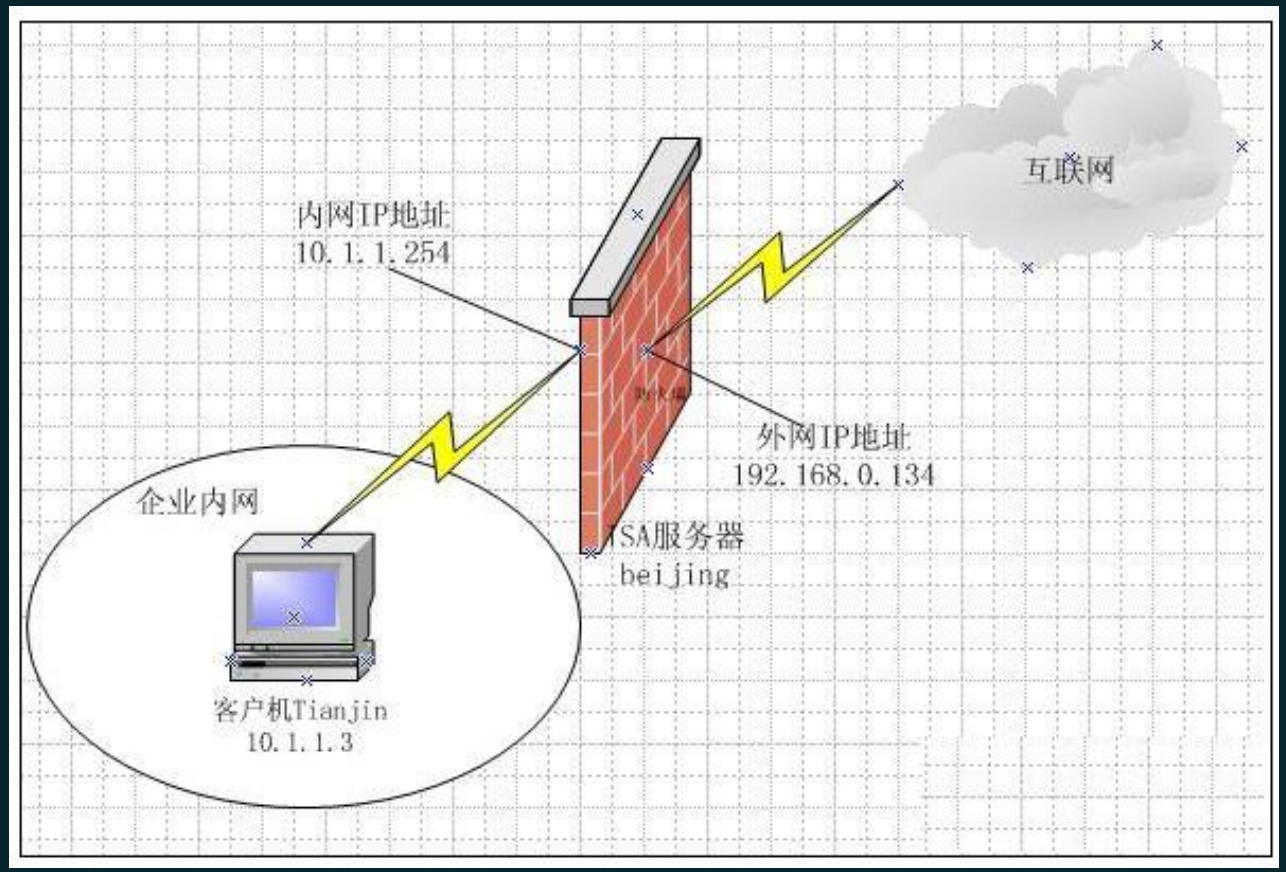
6 一层VPN的溯源

# 怎么定义特种木马?

# 特种木马对网络的穿透性

1. 穿透ISA代理及硬件代理
2. 绕过流量监控及地址检测
3. 使用多协议进行内容穿透
4. 协议加密穿透IPS/IDS
5. 使用隧道穿透单机防火墙

# 穿透代理


互联网
内网IP地址
10.1.1.254
外网IP地址
192.168.0.134
企业内网
ISA服务器
beijing
客户机Tianjin
10.1.1.3

# 绕过流量监控和恶意地址检测

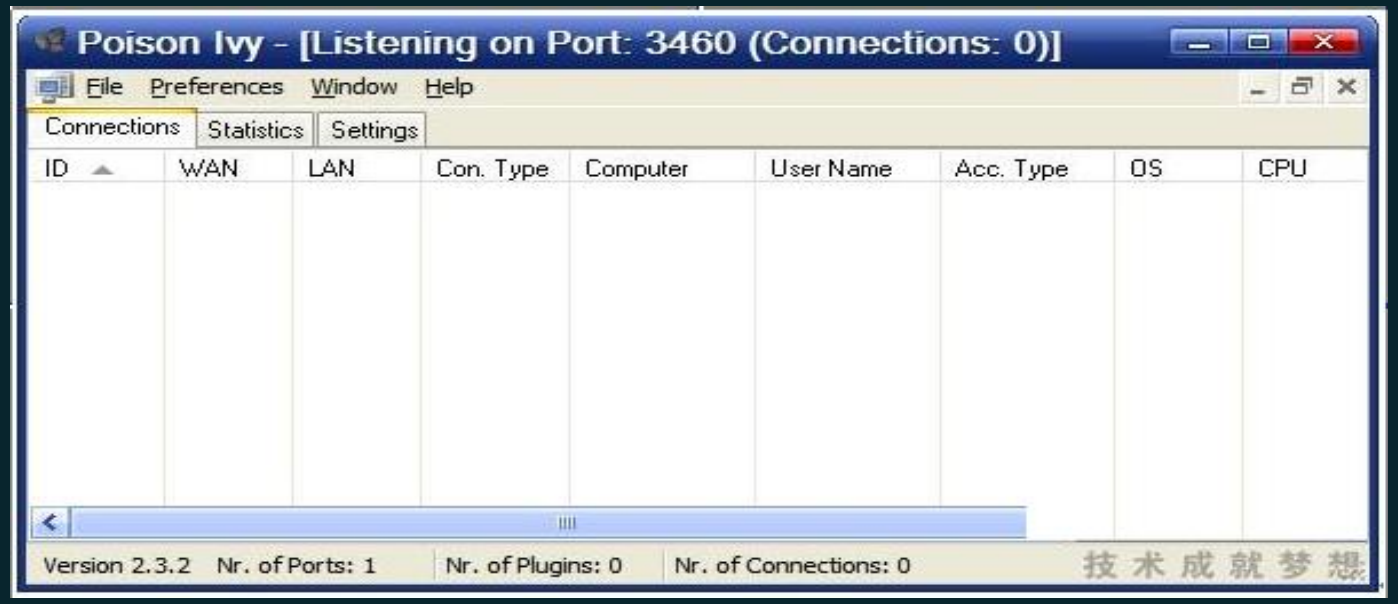


把数据传到公共网络逃避恶意地址检测和流量检测

# 采用多种协议穿透


一般会使用应用协议如HTTP DNS 等

# 协议加密绕过IPS/IDS防火墙




一般公开的RAT程序通信特性会被加入规则库

# 插入白名单程序绕单机防火墙


注入防火墙默认允许通讯的进程

# 与杀毒软件的对抗

1. 对抗虚拟机检测
2. 对抗启发式检测
3. 目前杀软的软肋

# 对抗虚拟机检测

1. 搜索虚拟环境中的进程，文件系统，注册表
2. 搜索虚拟环境中的内存
3. 搜索虚拟环境中的特定虚拟硬件
4. 搜索虚拟环境中的特定处理器指令和功能

# 对抗启发式检测

把功能做成shellcode或者使用动态获取api针对启发式面杀效果好
或者把恶意代码糅合和庞大的开源项目也会有好的逃逸效果。

# 目前杀软的软肋

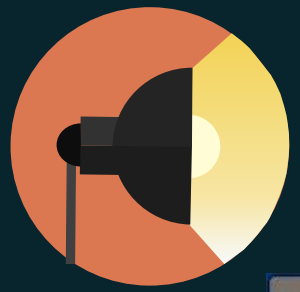

恶意程序利用第三方的白名单程序是杀毒软件的一个软肋

# 特种木马的溯源

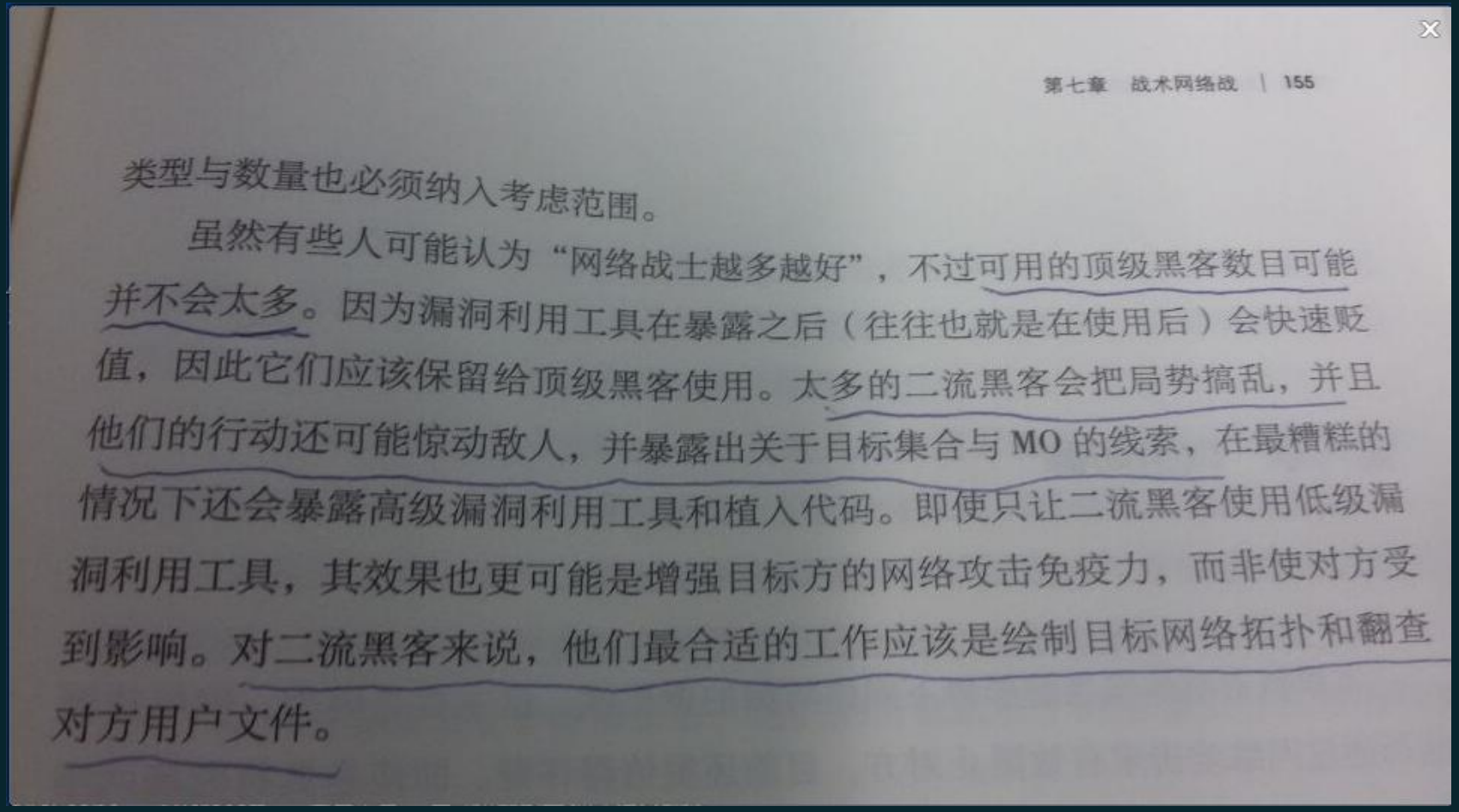
1. 我们的对手是谁
2. 如何发现特种木马
3. 基于二进制的分析
4. 基于IP的分析
5. 基于蜜罐的分析
6. 一层VPN的溯源

# 溯源之难

1. 隐藏成本底
2. VPN盛行，国与国之间协调困难



# 我们的对手是谁？



第七章　战术网络战 | 155

类型与数量也必须纳入考虑范围。

虽然有些人可能认为“网络战士越多越好”，不过可用的顶级黑客数目可能并不会太多。因为漏洞利用工具在暴露之后（往往也就是在使用后）会快速贬值，因此它们应该保留给顶级黑客使用。太多的二流黑客会把局势搞乱，并且他们的行动还可能惊动敌人，并暴露出关于目标集合与 MO 的线索，在最糟糕的情况下还会暴露高级漏洞利用工具和植入代码。即便只让二流黑客使用低级漏洞利用工具，其效果也更可能是增强目标方的网络攻击免疫力，而非使对方受到影响。对二流黑客来说，他们最合适的工作应该是绘制目标网络拓扑和翻查对方用户文件。

引用兰德报告的一段话

# 如何发现特种木马

1. 有大量样本数据

2. 对大量数据的甄别能力

# 基于调试信息的溯源

```
Hash: 3b01677582e7a56942a91da9728c6251- financial_report.exe
Debug Path: C:\Users\whg\Desktop\Plug\FastGui(LYT)\Shell\Release\Shell.pdb
Compilation date: 6/17/2012 16:44:58

Hash: 60ee900d919da8306b7b6dbe7e62fee49f00ccf141b2e396f5a66be51a00e34f
Debug Path: C:\Documents and Settings\whg\\Plug\FastGui(LYT)\Shell\Release\Shell.pdb
Compilation date: 2012-03-12 07:04:12

Hash: c00cd2dcddbb24383a3639ed56e68a24dc4561b1248efa4d53aa2b68220b4b2a
Debug Path: C:\Users\whg\Desktop\Plug\FastGui(LYT)\Shell\Release\Shell.pdb
Compilation date: 3/12/2012 14:23:58
```

编译器会记录你的信息

# 基于IP的一个溯源案例

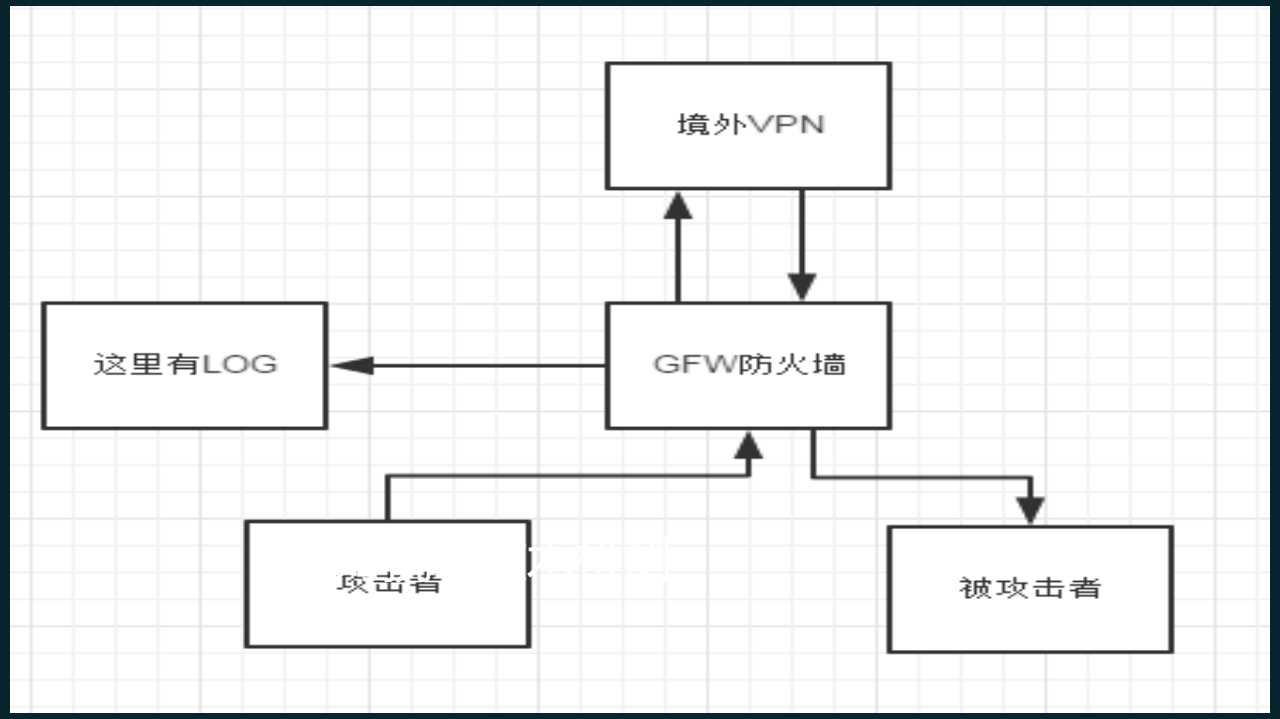
有一个服务商的名字为DomainTools它拥有12年的历史记录包括对域名的所有权，域名注册记录，托管数据，截图和其他DNS记录等信息。

# 基于蜜罐的分析

蜜罐溯源的小思路

在各种文档中插入一些引用网络的资源，如图片。

# 一层VPN的溯源




网络出入口是否有日志可查是关键所在

# 基于日志的分析

日志分析的难点

主要在于，攻击指纹确定以及大量日志联动分析。

日志分析案例

例如 攻击者在攻击过程中VPN出现断线情况。

# 谢谢观看

天融信

我的联系方式qq: 121  121  606