

软件安全—恶意代码机理与防护

C11 恶意软件样本捕获与分析

武汉大学国家网络安全学院 梁玉

liangyu@whu.edu.cn

本讲提纲

- 11.1 恶意软件样本捕获方法
 - 11.2 恶意软件载体
 - 11.3 恶意软件样本分析方法
 - 11.4 恶意软件样本分析工具
-

本讲提纲

- 11.1 恶意软件样本捕获方法
 - 11.2 恶意软件载体
 - 11.3 恶意软件样本分析方法
 - 11.4 恶意软件样本分析工具
-

11.1 恶意软件捕获方法

- ❑ 蜜罐
 - ❑ 用户上报
 - ❑ 云查杀平台
 - ❑ 诱饵邮箱
 - ❑ 样本共享
-

蜜罐

□ 蜜罐（Honeypot）

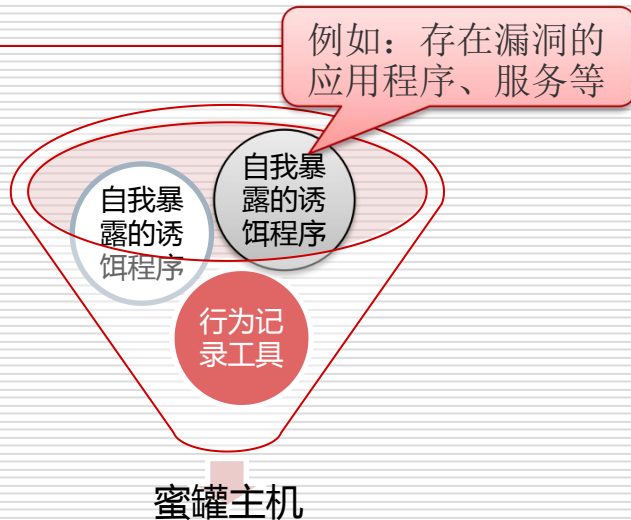
- 通常是指未采取安全防范措施、并且将模拟的程序漏洞主动暴露在网络中的计算机。

□ 特点

- 与一般计算机不同，其内部运行着多种多样特殊用途的“自我暴露程序”和行为记录程序
- 引诱恶意软件在蜜罐内更加充分的运行，并记录下其行为。

□ 工作模式

- 被动型蜜罐
- 主动型蜜罐



蜜罐

□ 被动型蜜罐

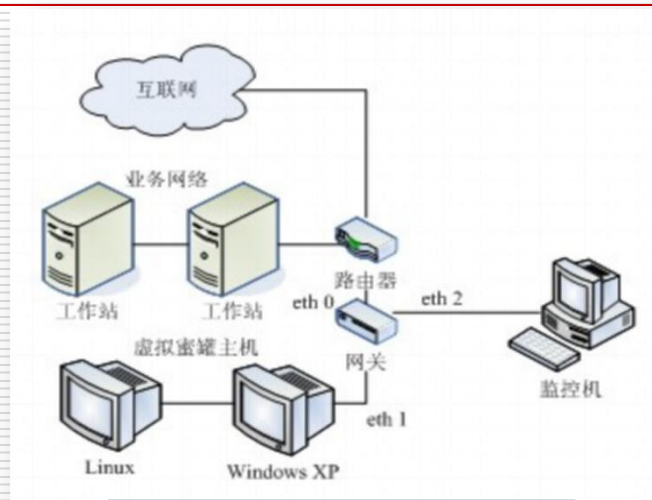
- 在蜜罐主机上模拟漏洞利用攻击所需的**部分服务**，**通过被动的方式**捕获主动传播类型的恶意软件，如蠕虫等

优点

- 捕获漏洞利用样本信息
- 获态

缺点

- 被动式交互、效率低
- 大规



被动型蜜罐的部署示意图

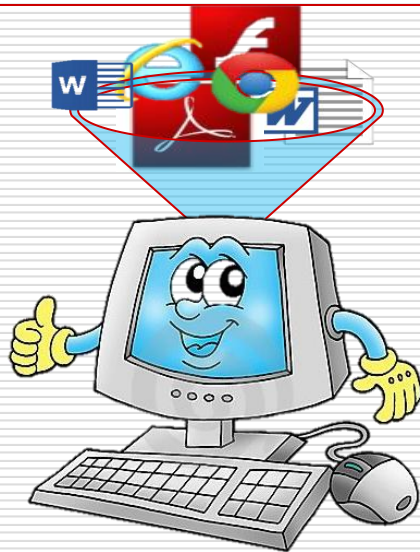
蜜罐

□ 主动型蜜罐

■ 主动型蜜罐的出现

- 针对客户端软件的恶意软件更为频繁，如web浏览器等
- 恶意软件的传播更具针对性和定向性，降低了传统被动型蜜罐的工作效率
- 需要仿真和模拟更真实的运行环境、更多的行为交互。

■ 主动型蜜罐也称作客户端蜜罐、沙箱

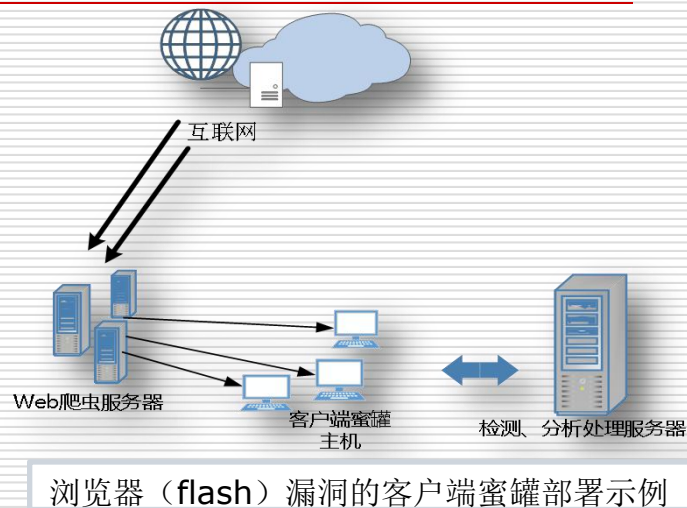


蜜罐

□ 主动型蜜罐——实现思路

- Step1:通过爬虫等主动获取潜在的恶意软件(载体)
- Step2:将其在蜜罐主机内打开、运行，并模拟进行交互
- Step3:根据运行特征，发现和收集漏洞利用信息和恶意软件样本。

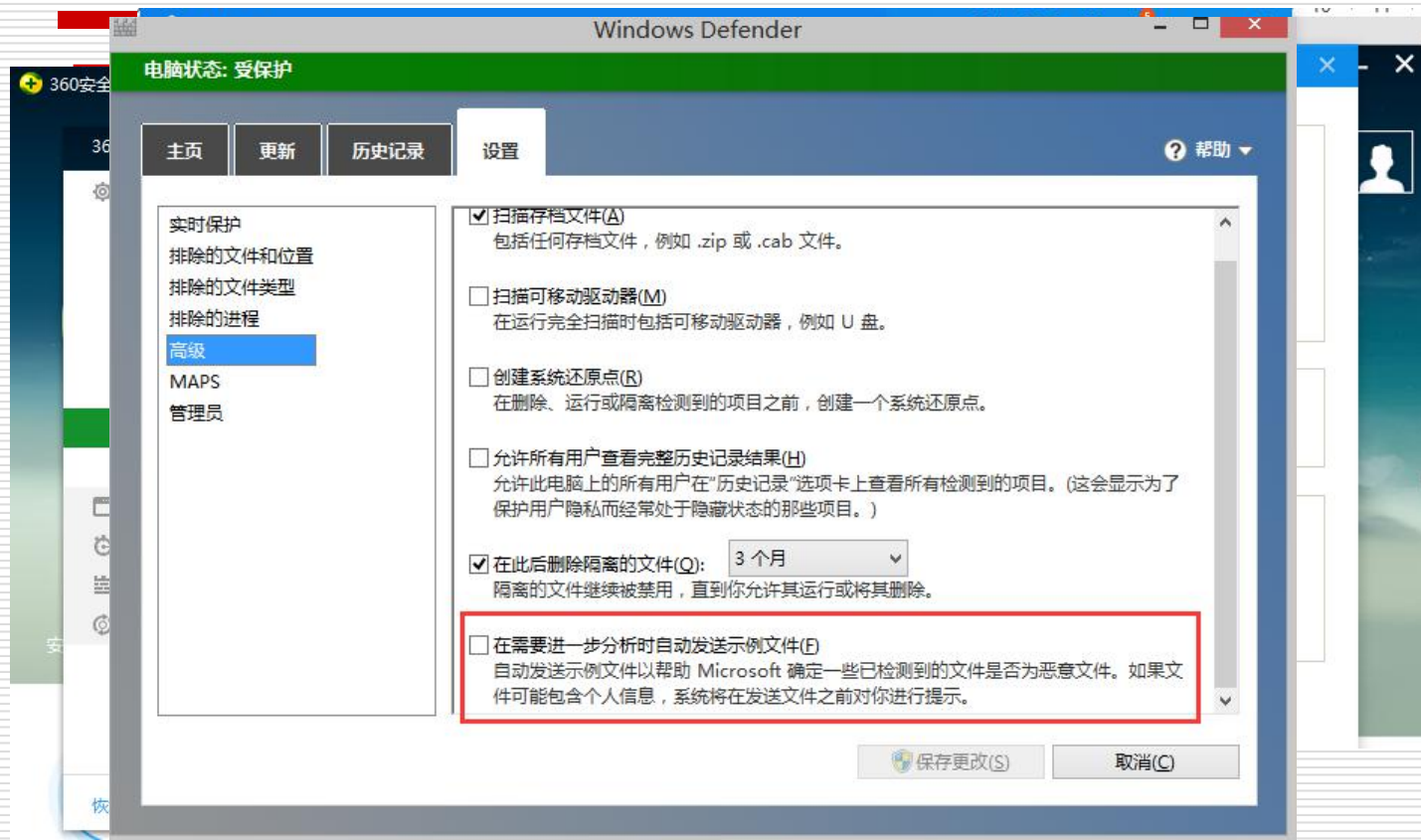
- 云计算和虚拟化技术使得设计和部署更为真实、更加先进的客户端蜜罐环境变得更加容易和低成本



用户上报

- 由个人用户在使用电脑过程中，发现恶意样本后主动上报给安全研究人员或机构
 - 上报途径
 - 安全产品的官方论坛
 - 产品客户端上传接口
 - 在线分析平台，如VirusTotal、Anubis等
 - 特点
 - 用户上报的样本通常较新，有一定的代表性
-

云查杀平台上传



云查杀平台上传

□ 云查杀获取样本的利与弊

好处

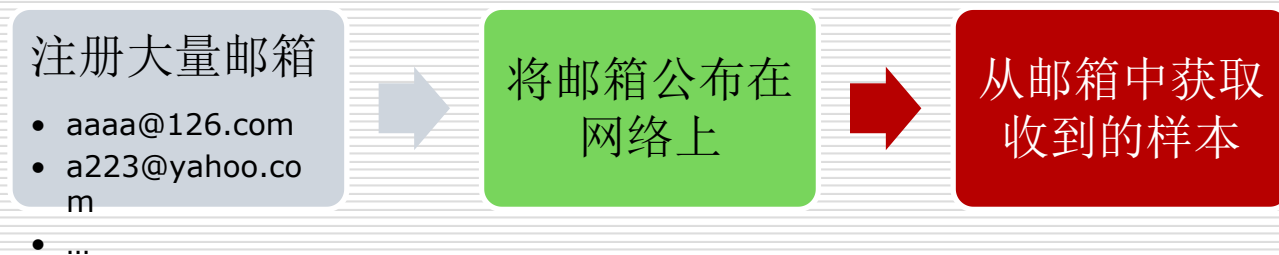
- 样本空间广泛，可大大提高恶意软件查杀的能力

弊端

- 易造成个人隐私或企业重要数据的泄露
-

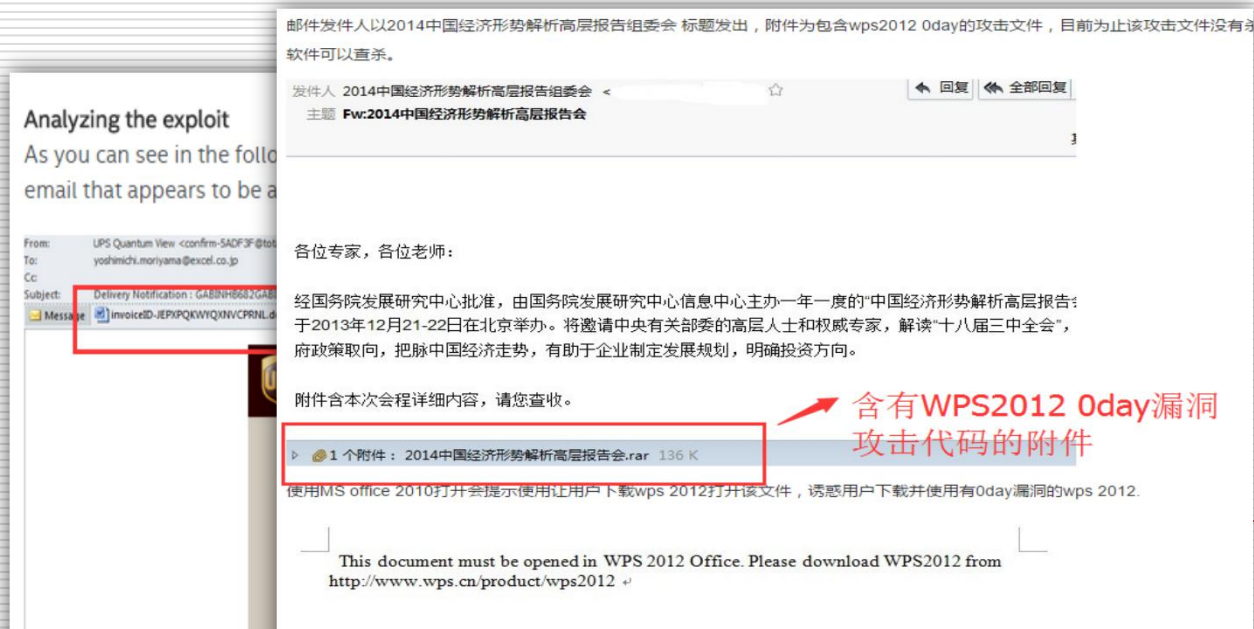
诱饵邮箱

- ❑ 在21世纪初，很多计算机病毒都使用电子邮件传播，用户在打开电子邮件或其附件时中毒。
- ❑ 通过诱饵邮箱捕获样本的工作流程

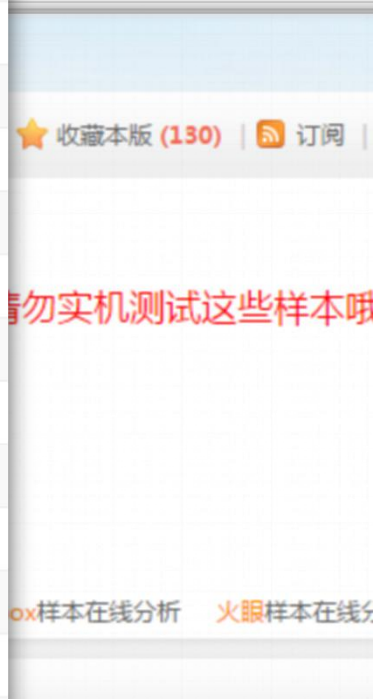
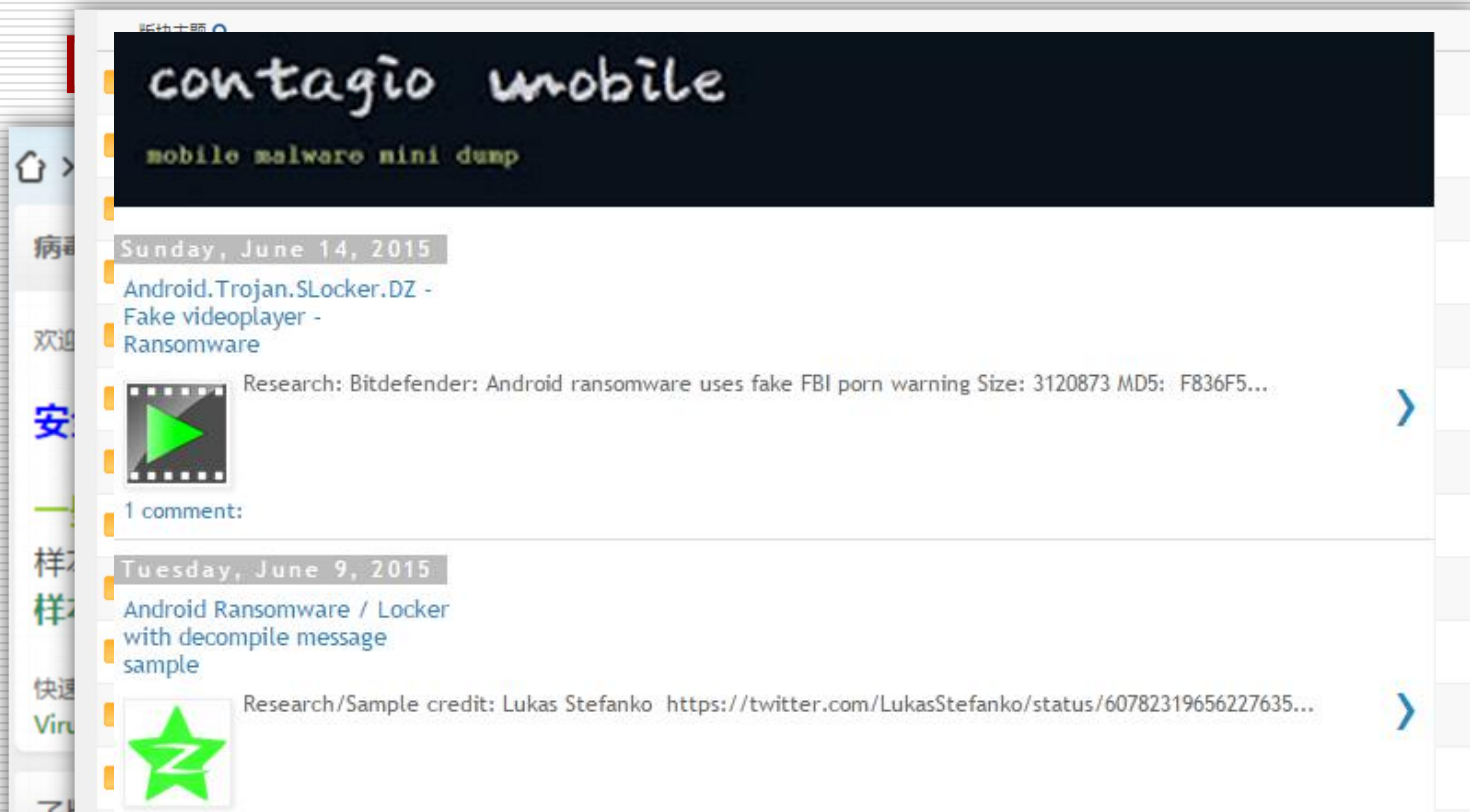


诱饵邮箱

- 在针对个人的各类APT攻击行为中，电子邮箱也是主要入侵渠道之一。因此，诱饵邮箱依然可以发挥重要作用。



样本交流



参考资料

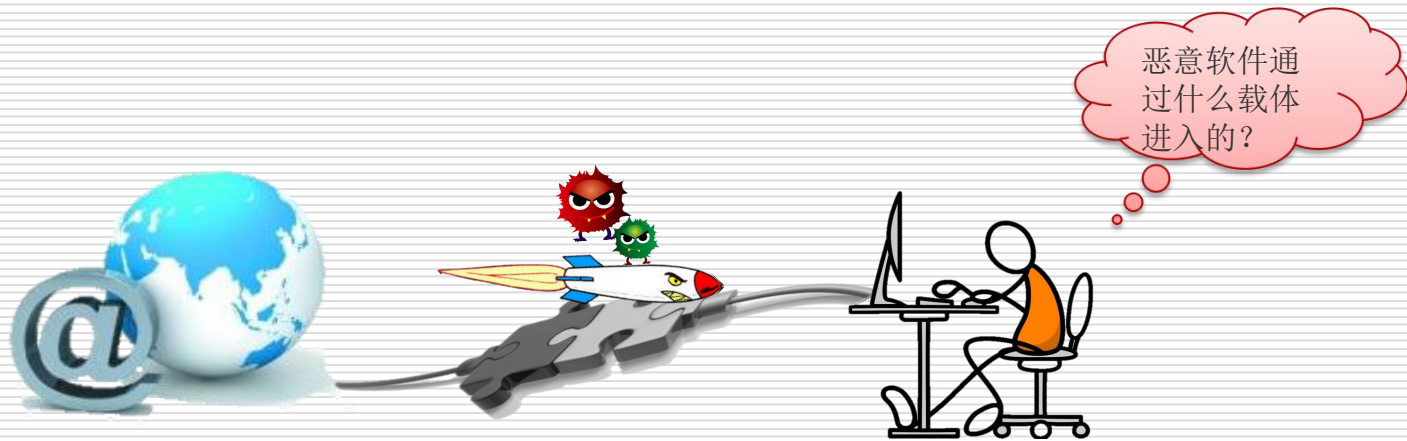
- ❑ Niels Provos Thorsten Holz. 虚拟蜜罐：从僵尸网络追踪到入侵检测
 - ❑ RTF Attack Takes Advantage of Multiple Exploits
<https://blogs.mcafee.com/mcafee-labs/rtf-attack-takes-advantage-of-multiple-exploits>
 - ❑ 利用wps 2012/2013 0day针对中国政府部门的定向攻击
http://blog.vulnhunt.com/index.php/2013/12/03/target_attack_with_wps2012_0day_in_the_wild/
-

本讲提纲

- 11.1 恶意软件样本捕获方法
 - 11.2 恶意软件载体
 - 11.3 恶意软件样本分析方法
 - 11.4 恶意软件样本分析工具
-

11.2 恶意软件载体

- ❑ 在彻底清除主机内的恶意软件时，需要定位恶意软件的来源、传播方式和存在形式，即载体。
- ❑ 不同类型的恶意软件有不同的传播方式与存在形式



11.2 恶意软件载体

□ 文件感染型病毒



向win32.dll插入新的代码节来存储病毒代码

的文件字
于文件的
数据云做修改。
的存储载体。

引导扇区事先进行过校验和计
此类恶意软件。

区

11.2 恶意软件载体

□ 蠕虫、木马类恶意软件

□ 植入方式

- 通常不感染可执行文件，而是和正常软件一样“安装”到系统中
- 安装过程比较隐蔽，多通过漏洞利用直接进入目标主机

□ 恶意软件定位

- 系统出现异常后，通过专业手段分析系统启动项、新启动的进程、线程，来发现和定位这类恶意软件样本
-

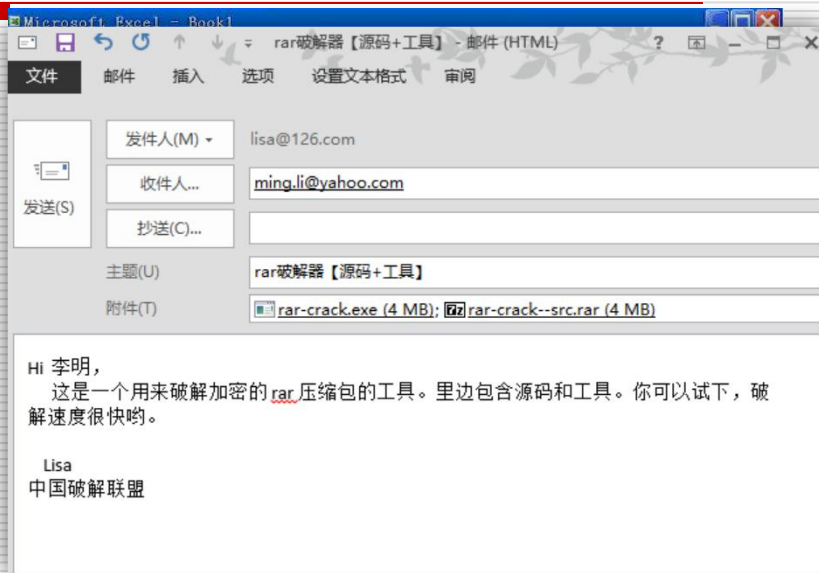
11.2 恶意软件载体

□ 宏病毒

- 可疑文档或Word、Excel、PowerPoint的模板文件是这类病毒的主要载体。

□ 电子邮件类

- 电子邮件的正文，特别是附件（如exe、com、scr，vb、bat等文件），通常是病毒的主要载体。



11.2 恶意软件载体

□ 脚本类恶意代码

□ 通过脚本触发漏洞

- 通过支持脚本的软件的漏洞传播恶意代码一种常见的且十分有效的方式。
 - 用于触发漏洞的恶意代码通常藏匿于脚本中。
 - 例如，通过浏览器中JavaScript、VBScript触发浏览器漏洞、或者通过Flash文件中的ActionScript触发漏洞，然后编码在脚本中的恶意代码。
-

11.2 恶意软件载体

□ 脚本类恶意代码

□ 通过网页中脚本直接传播

- 直接在网页中插入恶意的脚本代码。
 - 例如：采用VBScript编写的“新欢乐时光”向邮件客户端的信纸中插入恶意脚本代码。当发送邮件时病毒会附在邮件中。会感染html/htm、jsp、vbs、php、asp等格式的文件
-

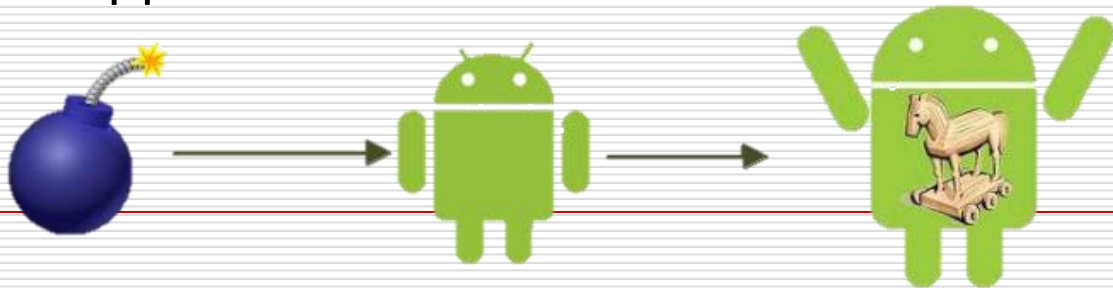
11.2 恶意软件载体

□ 扩展：应用程序重打包（Android App）

□ Android App

- 具有容易被逆向分析、修改后可以再次打包为可运行App的特点
- 因此，以流行App为载体、向其中插入恶意代码后重打包，这种方式是Android恶意代码传播的一个重要方式。

- 完整性校验：与原版App进行对比，即可定位出插入到重打包app中的恶意代码。



11.2 恶意软件载体

□ 恶意软件清除

- 正常情况下，可疑软件都可以被定位
 - 如果病毒采用了rootkit功能，则需要采用相关rootkit 检测工具进行检测和清除。
-

本讲提纲

- 11.1 恶意软件样本捕获方法
 - 11.2 恶意软件载体
 - 11.3 恶意软件样本分析方法
 - 11.4 恶意软件样本分析工具
-

恶意软件样本分析

恶意软件样本分析的目的



恶意软件样本分析方法

恶意软件样本分析的目的

□ 概述

- 样本分析是安全研究人员最基本的一项基本技能。
 - 通过样本分析：
 - 理解其工作机理和行为特征
 - 实现或完善相应的安全检测机制
 - 实现对已有恶意软件和未知恶意软件的防御、检测。
-

恶意软件样本分析的目的

□ 通过对样本的基本分析，解答如下问题：

- 程序有哪些破坏功能？
 - 程序的破坏功能是如何实现的？
 - 程序有哪些网络活动、其活动特征是什么样的？
 - 程序是如何实现系统驻留和自启动的？
 - 程序是否感染系统或其他程序，或网络中的其它主机？
 - 程序是如何进入系统的？
 - ...
-

恶意软件样本分析的目的

- 出于取证分析、持续威胁的追踪和溯源，还需要思考：
 - 程序编写者具备哪些编程习惯和特征？
 - 程序使用什么典型攻击手法来攻击主机？
 - 程序反映出攻击者的技术水平如何？
 - 攻击者可能是什么样的团体或组织，存在哪些控制的行为特征模式？
 - 该程序是否与其它恶意软件存在关联？
 - ...
-

恶意软件样本的分析方法

□ 常用分析方法

在线分析

- 在线病毒扫描
- 在线行为分析

本地静态分析

- 加壳检测与脱壳
- 反汇编/反编译
- 资源分析

本地动态分析

- 快照对比分析
- 行为监控分析
- 调试跟踪
- 网络监控分析
- 运行环境仿真

网络交互的动态分析

- 网络连接选择
 - 网络交互环境仿真
 - 数据包捕获分析
-

恶意软件样本的分析方法

□ 运行环境仿真

- 时间模拟
- 文件资源模拟
- 对抗反虚拟机
- 对抗反调试

□ 网络交互环境仿真

- DNS构造
- IP地址分析和模拟
- 服务器模拟和数据响应模拟

□ 行为监控分析

- 关注文件、注册表、进程、网络、内存等操作

恶意软件样本的分析方法

□ 方法选择

□ 一般思路：粗粒度分析 → 针对性的细粒度分析

粗粒度分析

- 了解恶意软件的恶意行为
- 在线行为分析、快照比对、行为监控、粗粒度的资源分析等方法

细粒度分析

- 有针对性的研究恶意软件的功能实现、入侵细节、潜在威胁等
- 静态反汇编、动态调试分析、**API**监控、环境仿真等方法

本讲提纲

- 11.1 恶意软件样本捕获方法
 - 11.2 恶意软件载体
 - 11.3 恶意软件样本分析方法
 - **11.4 恶意软件样本分析工具**
-

11.4 恶意软件样本分析工具

- 常用分析工具介绍
 - 恶意软件分析报告
 - 恶意软件样本分析实例
-

常用分析工具

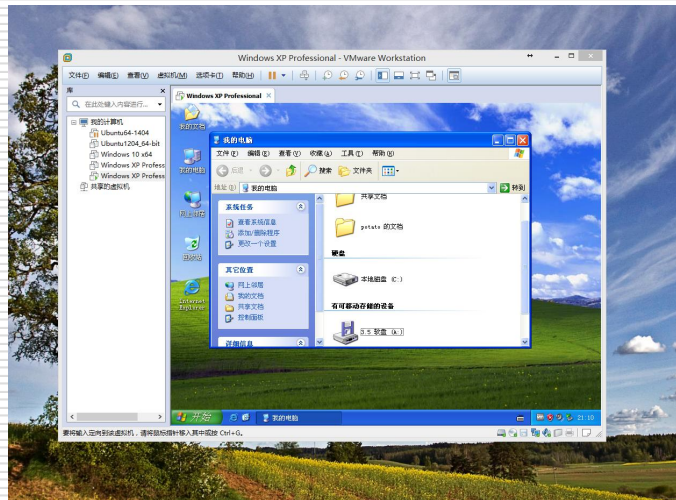
□ 虚拟机环境——提供样本运行环境

- 使用虚拟机软件将一台物理计算机硬盘和内存的一部分以及其它相关硬件资源分享出来，从而虚拟出若干计算机，每台计算机可运行单独操作系统。
 - 虚拟机中的系统与物理主机系统相互隔离，虚拟机之间相互隔离。
 - 常用虚拟机软件：VMWare、Virtual PC、Virtual Box等
-

常用分析工具

□ 虚拟机环境

- 在虚拟机环境分析恶意软件样本，防止对物理主机的感染和破坏
- 右图是虚拟机中运行的Windows XP



常用分析工具

□ 系统监控

- 监控样本运行期间的行为和对系统的改变
- Windows Sysinternals Suite是一套针对Windows系统的监控、分析工具。包含了ProcessMonitor、ProcessExplorer、Autoruns等很多有用工具

进程监控

文件监控

注册表监控

内核监控

网络连接分析

系统启动项分析

系统完整性检测

...

常用分析工具

□ 系统监控——进程监控

■ Process Explorer

进程树

句柄或
模块

The screenshot displays the Windows Task Manager application, showing a list of running processes and their associated loaded modules.

Process List:

Process	CPU	Private	Working	PID	Description	Company Name
System Idle Process	0.00	0 K	0 K	0		
System	0.10	47,136 K	2,704 K	4		
smss.exe	<...	300 K	1,068 K	360	Windows 会话管理器	Microsoft Corp...
csrss.exe	<...	1,852 K	5,008 K	456	Client Server R...	Microsoft Corp...
init.exe	<...	576 K	4,260 K	4,260	Windows 注册表	Microsoft Corp...
services.exe	<...	3,428 K	6,832 K	696	服务和控制管理器	Microsoft Corp...
svchost.exe	<...	6,488 K	13,336 K	728	Windows 服务主进程	Microsoft Corp...
chime.exe	<...	8,536 K	40,348 K	2533	Microsoft TME	Microsoft Corp...
SkyDrive.exe	11,952 K	15,540 K	3768	OneDrive Sync R...	Microsoft Corp...	
SettingSyncHost.exe	10,336 K	4,092 K	3404	Host Process fo...	Microsoft Corp...	
explorer.exe	4,284 K	2,648 K	310	腾讯QQ多语言中...	Tencent	
explorer.exe	30,332 K	50,120 K	3184	Windows 资源管理器	Microsoft Corp...	
POWERCFG.EXE	16,652 K	45,508 K	3648	Windows 电源管理...	Microsoft Corp...	
WINWORD.EXE	59,860 K	163,640 K	190	Microsoft Power...	Microsoft Corp...	
WordPrvSE.exe	372,216 K	349,280 K	5784	Microsoft Word	Microsoft Corp...	
svchost.exe	1,948 K	6,400 K	1115	WMI Provider Host	Microsoft Corp...	
ati6xx64.exe	6,016 K	10,780 K	772	Windows 设备主进程	Microsoft Corp...	
ati6xx64.exe	732 K	3,316 K	888	AMD External Ev...	AMD	
ati6xx64.exe	2,236 K	8,532 K	3143	AMD External Ev...	AMD	
audiodg.exe	0.01	19,190 K	25,064 K	913	Windows 服务主进程	Microsoft Corp...
audiodg.exe	0.05	7,056 K	10,112 K	4643	Windows 音频设备	Microsoft Corp...

Loaded Modules:

Name	Description	Company Name	Path
gdi32.dll	GDI Client DLL	Microsoft Cor...	C:\Windows\System32\gdi32.dll
kernel32.dll	Windows NT 基本 AP...	Microsoft Cor...	C:\Windows\System32\kernel32.dll
kernelBase.dll	Windows NT 基本 AP...	Microsoft Cor...	C:\Windows\System32\kernelBase.dll
locale.nls			C:\Windows\System32\locale.nls
advapi32.dll	Windows NT CRT DLL	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	Microsoft Windows ...	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	NSI User-mode inte...	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	NT 层 DLL	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	User Profile Basic...	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	远程过程调用运行时	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	Host for SCM/SDUL...	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	Security Support P...	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	多用户 Windows 用...	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	多用户 Windows 用...	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	Windows 启动应用程序	Microsoft Cor...	C:\Windows\System32\advapi32.dll
advapi32.dll	Windows Socket 2.0...	Microsoft Cor...	C:\Windows\System32\advapi32.dll

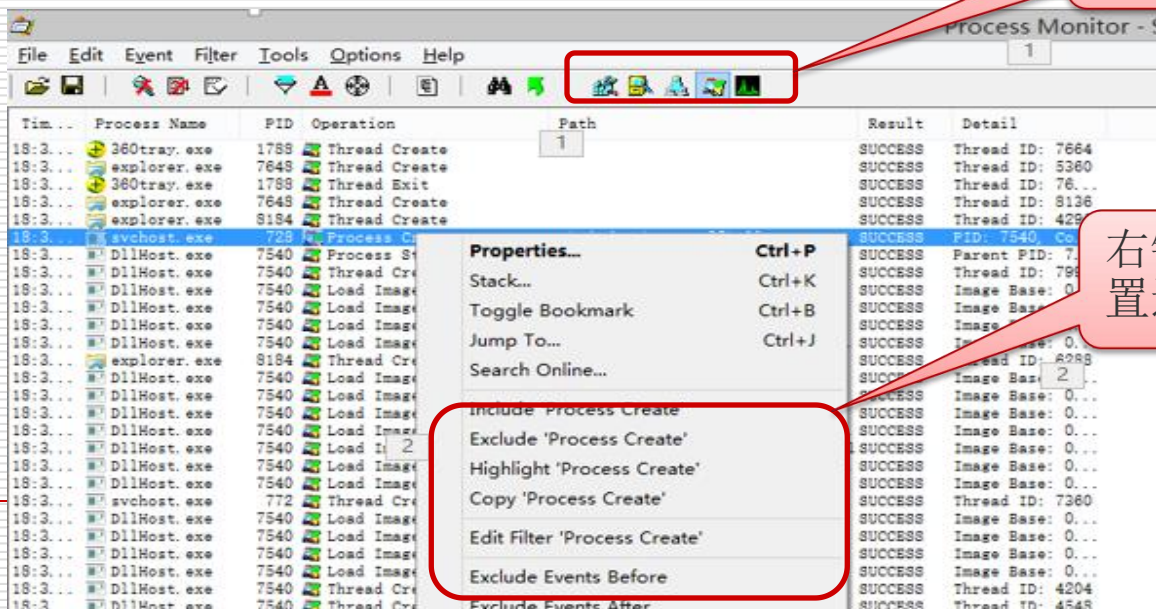
CPU Usage: 4.61% Commit Charge: 57.93% Processes: 97 Physical Usage: 45.21%

常用分析工具

□ 系统监控——进程监控

■ ProcessMonitor

设置过滤器，使其只
监控进程、线程行为

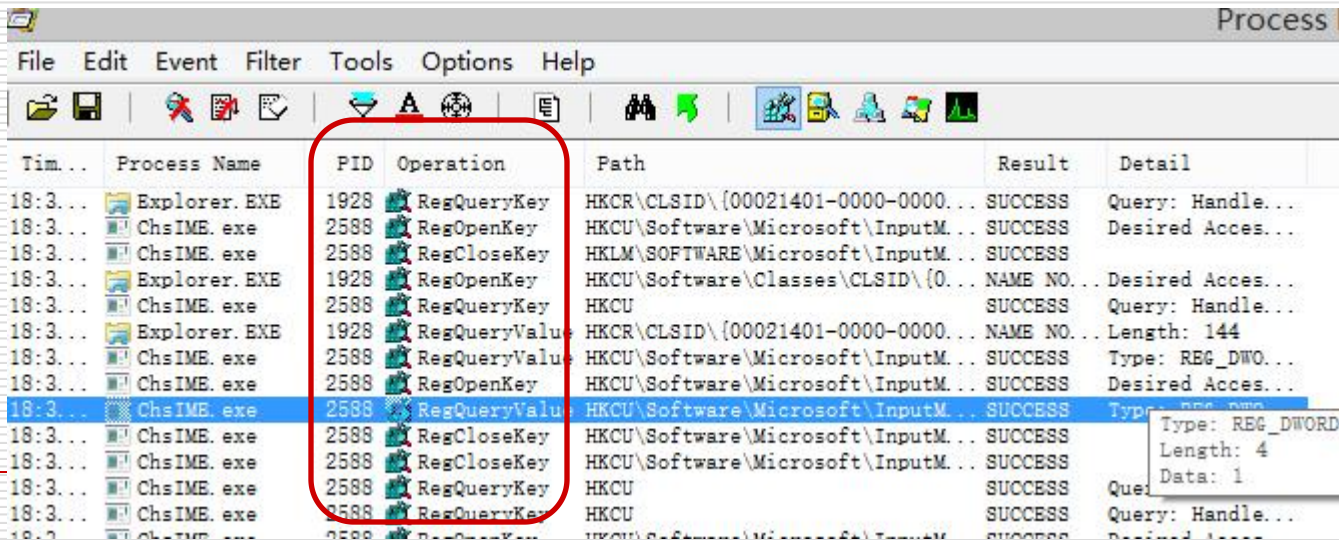


右键菜单设
置过滤模式

常用分析工具

□ 系统监控——注册表监控

- 设置ProcessMonitor过滤器，只监控注册表行为



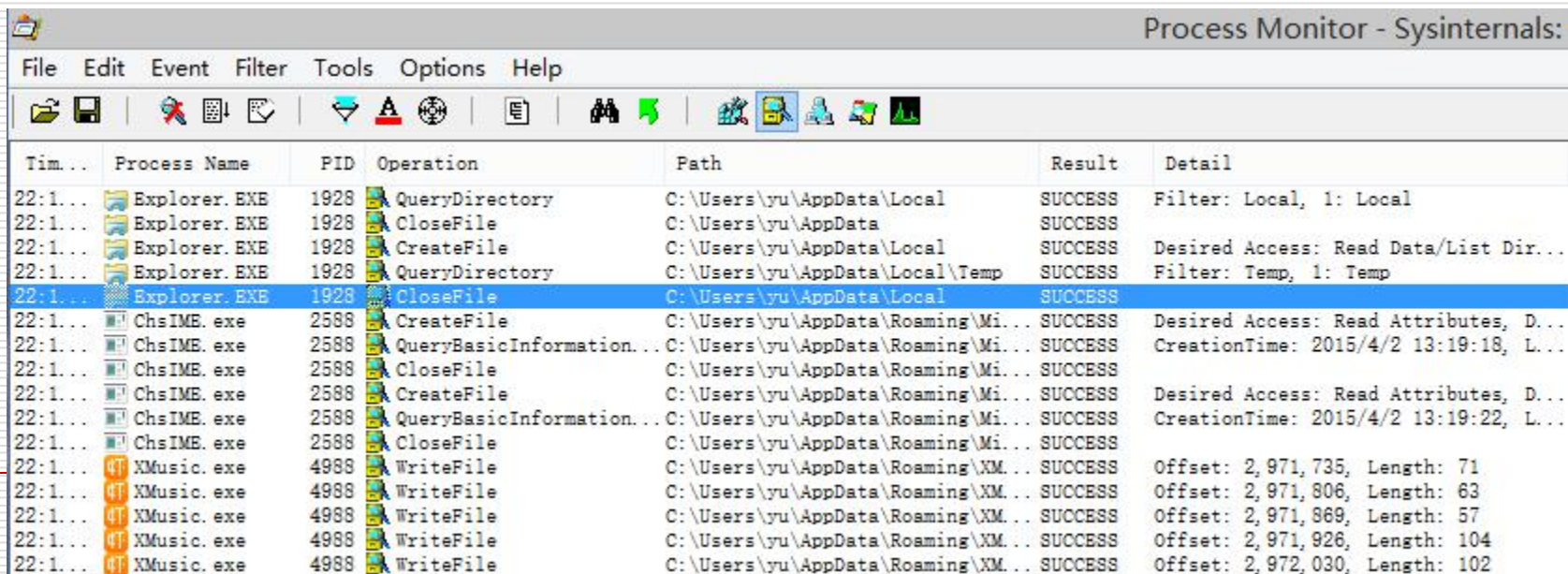
The screenshot shows the Process Monitor application window with the 'Filter' menu open. The 'Filter' menu is set to 'Registry Operations'. The main window displays a list of registry operations performed by various processes. A red circle highlights the 'Operation' column, and a tooltip is visible for the selected row.

Time	Process Name	PID	Operation	Path	Result	Detail
18:3...	Explorer.EXE	1928	RegQueryKey	HKCR\CLSID\{00021401-0000-0000...	SUCCESS	Query: Handle...
18:3...	ChsIME.exe	2588	RegOpenKey	HKCU\Software\Microsoft\InputM...	SUCCESS	Desired Acces...
18:3...	ChsIME.exe	2588	RegCloseKey	HKLM\SOFTWARE\Microsoft\InputM...	SUCCESS	
18:3...	Explorer.EXE	1928	RegOpenKey	HKCU\Software\Classes\CLSID\{0...	NAME NO...	Desired Acces...
18:3...	ChsIME.exe	2588	RegQueryKey	HKCU	SUCCESS	Query: Handle...
18:3...	Explorer.EXE	1928	RegQueryValue	HKCR\CLSID\{00021401-0000-0000...	NAME NO...	Length: 144
18:3...	ChsIME.exe	2588	RegQueryValue	HKCU\Software\Microsoft\InputM...	SUCCESS	Type: REG_DWO...
18:3...	ChsIME.exe	2588	RegOpenKey	HKCU\Software\Microsoft\InputM...	SUCCESS	Desired Acces...
18:3...	ChsIME.exe	2588	RegQueryValue	HKCU\Software\Microsoft\InputM...	SUCCESS	Type: REG_DWORD
18:3...	ChsIME.exe	2588	RegCloseKey	HKCU\Software\Microsoft\InputM...	SUCCESS	Length: 4
18:3...	ChsIME.exe	2588	RegCloseKey	HKCU\Software\Microsoft\InputM...	SUCCESS	Data: 1
18:3...	ChsIME.exe	2588	RegQueryKey	HKCU	SUCCESS	Query: Handle...
18:3...	ChsIME.exe	2588	RegQueryKey	HKCU	SUCCESS	Query: Handle...

常用分析工具

□ 系统监控——文件行为监控

■ 设置ProcessMonitor过滤器，只监控注册表行为

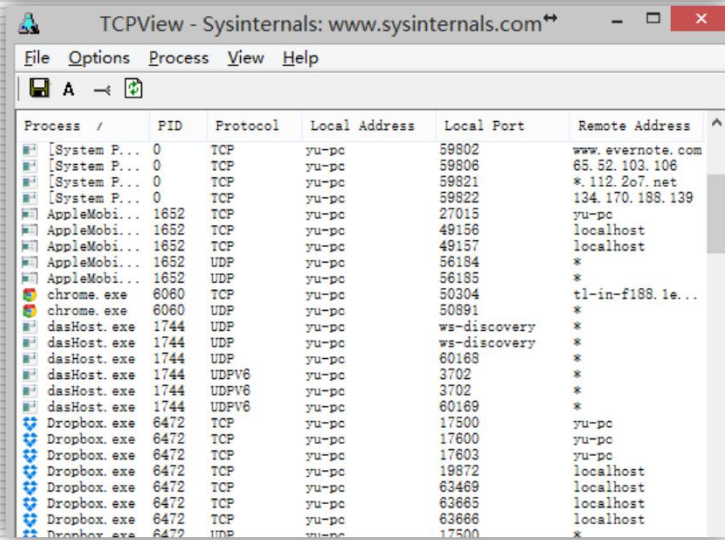


Tim...	Process Name	PID	Operation	Path	Result	Detail
22:1...	Explorer.EXE	1928	QueryDirectory	C:\Users\yu\AppData\Local	SUCCESS	Filter: Local, 1: Local
22:1...	Explorer.EXE	1928	CloseFile	C:\Users\yu\AppData	SUCCESS	
22:1...	Explorer.EXE	1928	CreateFile	C:\Users\yu\AppData\Local	SUCCESS	Desired Access: Read Data/List Dir...
22:1...	Explorer.EXE	1928	QueryDirectory	C:\Users\yu\AppData\Local\Temp	SUCCESS	Filter: Temp, 1: Temp
22:1...	Explorer.EXE	1928	CloseFile	C:\Users\yu\AppData\Local	SUCCESS	
22:1...	ChsIME.exe	2588	CreateFile	C:\Users\yu\AppData\Roaming\Mi...	SUCCESS	Desired Access: Read Attributes, D...
22:1...	ChsIME.exe	2588	QueryBasicInformation...	C:\Users\yu\AppData\Roaming\Mi...	SUCCESS	CreationTime: 2015/4/2 13:19:18, L...
22:1...	ChsIME.exe	2588	CloseFile	C:\Users\yu\AppData\Roaming\Mi...	SUCCESS	
22:1...	ChsIME.exe	2588	CreateFile	C:\Users\yu\AppData\Roaming\Mi...	SUCCESS	Desired Access: Read Attributes, D...
22:1...	ChsIME.exe	2588	QueryBasicInformation...	C:\Users\yu\AppData\Roaming\Mi...	SUCCESS	CreationTime: 2015/4/2 13:19:22, L...
22:1...	ChsIME.exe	2588	CloseFile	C:\Users\yu\AppData\Roaming\Mi...	SUCCESS	
22:1...	XMusic.exe	4988	WriteFile	C:\Users\yu\AppData\Roaming\XM...	SUCCESS	Offset: 2, 971, 735, Length: 71
22:1...	XMusic.exe	4988	WriteFile	C:\Users\yu\AppData\Roaming\XM...	SUCCESS	Offset: 2, 971, 806, Length: 63
22:1...	XMusic.exe	4988	WriteFile	C:\Users\yu\AppData\Roaming\XM...	SUCCESS	Offset: 2, 971, 869, Length: 57
22:1...	XMusic.exe	4988	WriteFile	C:\Users\yu\AppData\Roaming\XM...	SUCCESS	Offset: 2, 971, 926, Length: 104
22:1...	XMusic.exe	4988	WriteFile	C:\Users\yu\AppData\Roaming\XM...	SUCCESS	Offset: 2, 972, 030, Length: 102

常用分析工具

□ 系统监控——网络行为监控

- 使用系统命令netstat或ProtMon工具查看网络连接情况
- 使用TCPView或ProcessMonitor查看网络行为记录



The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu bar is a toolbar with icons for file operations and a search icon. The main area displays a table of active network connections.

Process /	PID	Protocol	Local Address	Local Port	Remote Address
[System P...	0	TCP	yu-pc	59802	www.evernote.com
[System P...	0	TCP	yu-pc	59806	65.52.103.106
[System P...	0	TCP	yu-pc	59821	*.112.2o7.net
[System P...	0	TCP	yu-pc	59822	134.170.188.139
AppleMobi...	1652	TCP	yu-pc	27015	yu-pc
AppleMobi...	1652	TCP	yu-pc	49156	localhost
AppleMobi...	1652	TCP	yu-pc	49157	localhost
AppleMobi...	1652	UDP	yu-pc	56184	*
AppleMobi...	1652	UDP	yu-pc	56185	*
chrome.exe	6060	TCP	yu-pc	50304	tl-in-f188.1e...
chrome.exe	6060	UDP	yu-pc	50891	*
dasHost.exe	1744	UDP	yu-pc	*	ws-discovery
dasHost.exe	1744	UDP	yu-pc	*	ws-discovery
dasHost.exe	1744	UDP	yu-pc	60168	*
dasHost.exe	1744	UDPV6	yu-pc	3702	*
dasHost.exe	1744	UDPV6	yu-pc	3702	*
dasHost.exe	1744	UDPV6	yu-pc	60169	*
Dropbox.exe	6472	TCP	yu-pc	17500	yu-pc
Dropbox.exe	6472	TCP	yu-pc	17600	yu-pc
Dropbox.exe	6472	TCP	yu-pc	17603	yu-pc
Dropbox.exe	6472	TCP	yu-pc	19872	localhost
Dropbox.exe	6472	TCP	yu-pc	63469	localhost
Dropbox.exe	6472	TCP	yu-pc	63665	localhost
Dropbox.exe	6472	TCP	yu-pc	63666	localhost
Dropbox.exe	6472	UDP	yu-pc	17500	*

COMODO 高级设置

一般设置

一般设置

安全设置

反病毒

反病毒

"防御+"

"防御+"

HIPS

HIPS

HIPS设置

HIPS

HIPS规则

HIPS

规则

规则

被保护的對象

被保护的對象

HIPS组

HIPS

沙盒

沙盒

Viruscope

Virus

防火墙

防火墙

文件评级

文件评级

COMODO HIPS



chromodo_updater.exe正在尝试修改一个被保护的文件或目录



chromodo_up...

chromodo_updater.exe 无法被识别并且它将修改C:\WINDOWS\Temp\Comodo LogsFolder\chromodo_updater.exe.log。在允许本次请求前,您必须确信chromodo_updater.exe是一个安全的应用程序。



允许

允许应用程序执行上面的操作



阻止

阻止应用程序执行上面的操作



信任为

由您选择一个规则并应用

☒ 记住我的选择

[展示活动](#)

取消

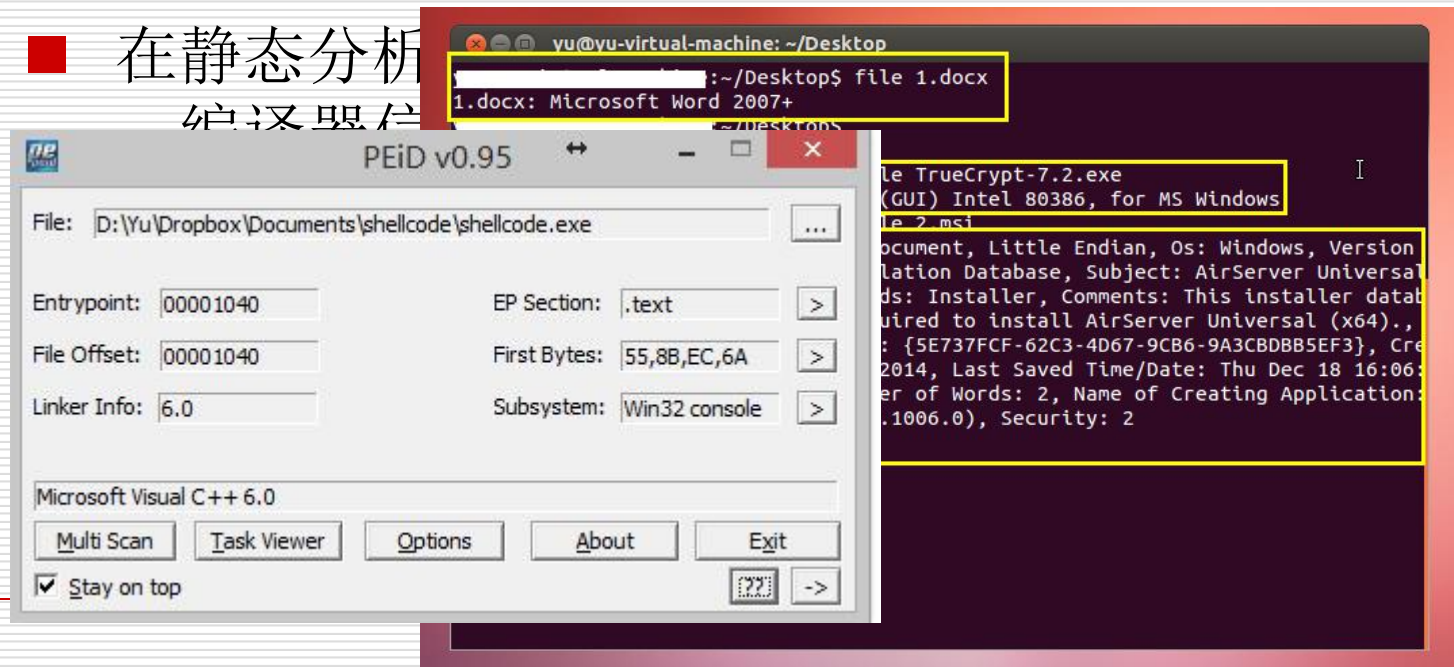
相

常用分析工具

□ 文件类型检测

■ 在静态分析

虚拟机中



常用分析工具

□ PE文件格式分析

■ 了解PE



入口点

常用分析工具

□ 静态反编译

- 将经过编译器编译后的机器码或字节码等还原成便于理解的语言形式的过程为反编译。

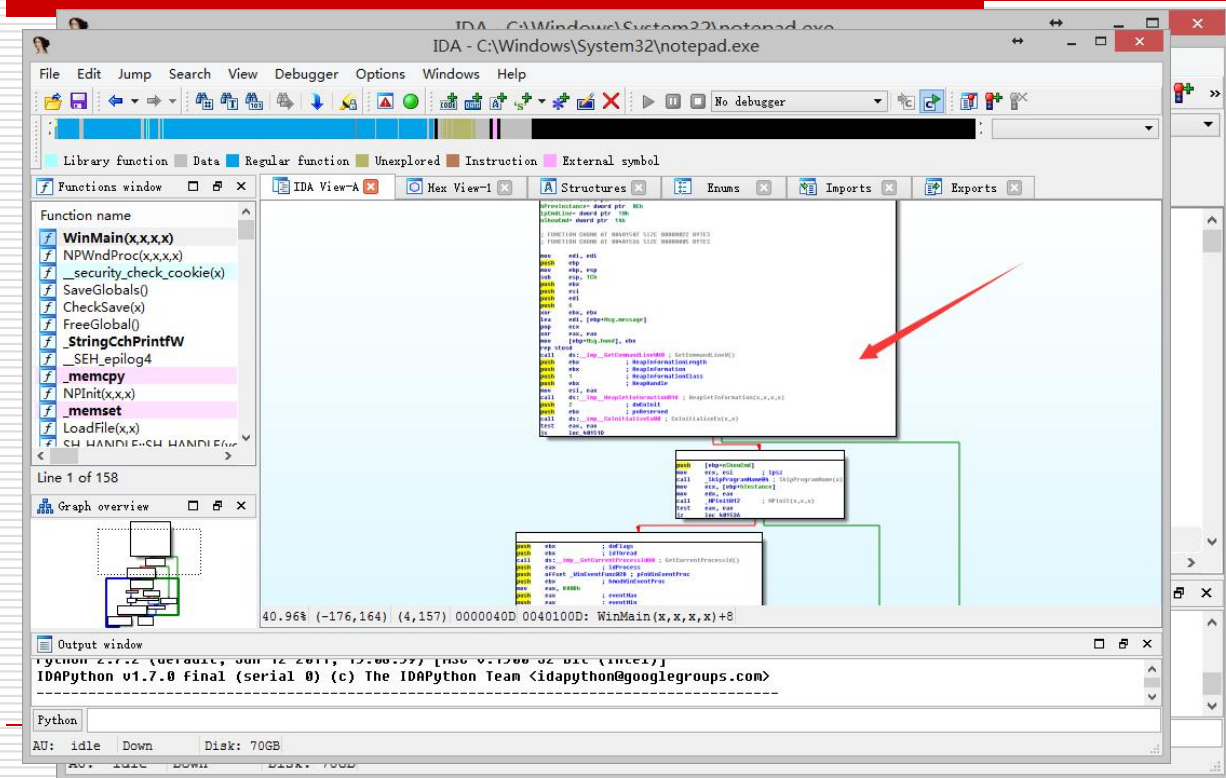
编译型
语言

源代码经过编译后
生成CPU可直接执行
的机器码的高级
语言

解释型
语言

源代码由解释器直
接解释执行；或编
译成字节码发布，
执行时由解释器解
释执行的高级语言

常用分析工具



常用分析工具

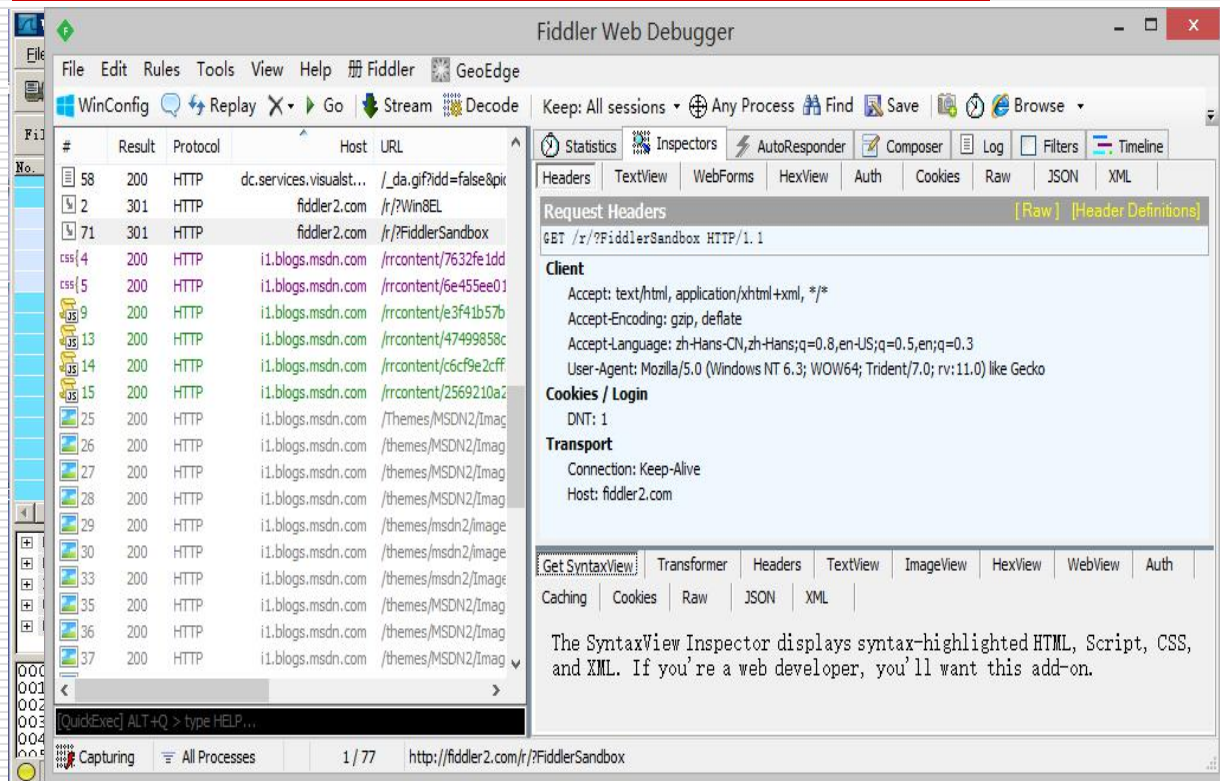
□ 动态调试

- 对目标程序进行运行时的单步跟踪，以进一步了解目标代码运行的细节，洞悉目标程序的运行机理。
 - OllyDbg、WinDBG、Immunity Debugger、GDB、IDA Pro等
-

DWS



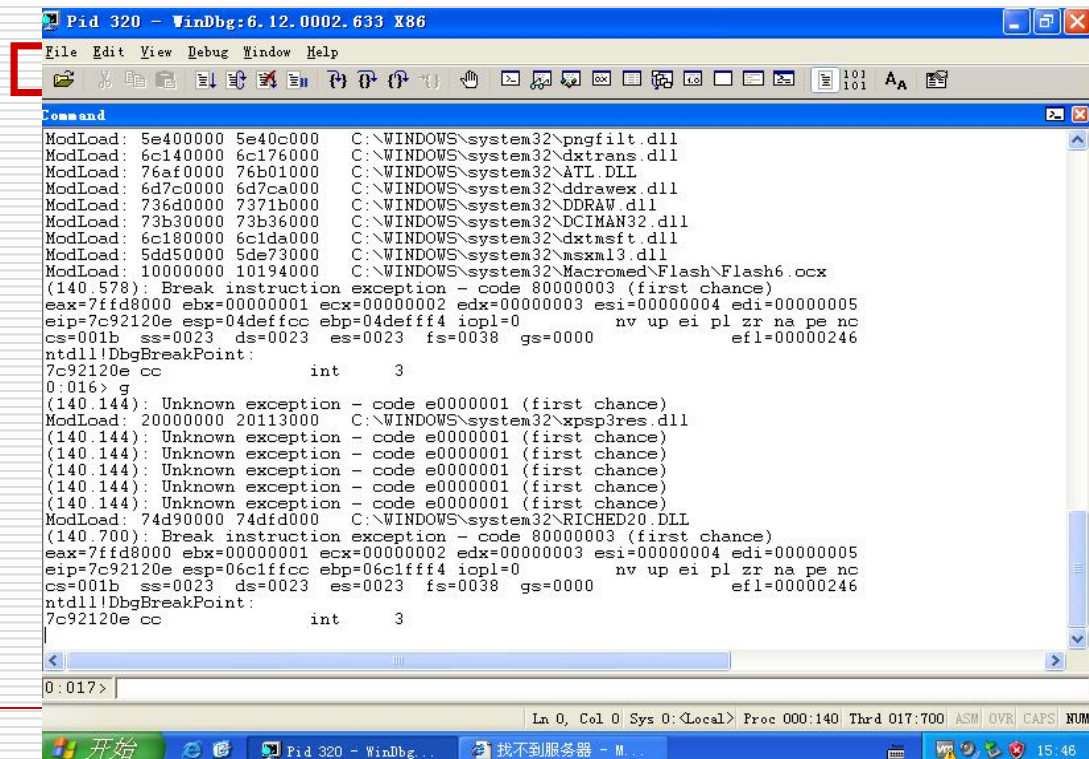
常用分析工具



以分析

居分析

常用分析工具



The screenshot shows the WinDbg 6.12.0002.633 X86 interface. The Command window displays the following output:

```
ModLoad: 5e400000 5e40c000 C:\WINDOWS\system32\pngfilt.dll
ModLoad: 6c140000 6c176000 C:\WINDOWS\system32\dxtrans.dll
ModLoad: 76af0000 76b01000 C:\WINDOWS\system32\ATL.DLL
ModLoad: 6d7c0000 6d7ca000 C:\WINDOWS\system32\ddrawex.dll
ModLoad: 736d0000 7371b000 C:\WINDOWS\system32\DDRAW.dll
ModLoad: 73b30000 73b36000 C:\WINDOWS\system32\DCIMAN32.dll
ModLoad: 6c180000 6c1da000 C:\WINDOWS\system32\dxtrans.dll
ModLoad: 5dd50000 5de73000 C:\WINDOWS\system32\msxml3.dll
ModLoad: 10000000 10194000 C:\WINDOWS\system32\Macromed\Flash\Flash6.ocx
(140.578): Break instruction exception - code 80000003 (first chance)
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=04deffcc ebp=04defff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc                int     3
0:016> g
(140.144): Unknown exception - code e0000001 (first chance)
ModLoad: 20000000 20113000 C:\WINDOWS\system32\xpssp3res.dll
(140.144): Unknown exception - code e0000001 (first chance)
(140.144): Unknown exception - code e0000001 (first chance)
(140.144): Unknown exception - code e0000001 (first chance)
(140.144): Unknown exception - code e0000001 (first chance)
(140.144): Unknown exception - code e0000001 (first chance)
(140.144): Unknown exception - code e0000001 (first chance)
ModLoad: 74d90000 74dfd000 C:\WINDOWS\system32\RICHED20.DLL
(140.700): Break instruction exception - code 80000003 (first chance)
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=06c1ffcc ebp=06c1fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc                int     3
0:017>
```

十分强大

调试支持较好

常用分析工具

□ 文件原始数据(RawData)分析

- 恶意软件样本的文件类型多种多样，有时候需要用特定类型格式解析文件、并用16进制进行查看特定字段数值。
 - 。
 - 例如在文件格式漏洞样本分析中，需查看flash文件（SWF）、pdf文件、mp3文件的特定字段
 - 工具：010Editor、UltraEdit、WinHex等
-

常用分析工具

010 Editor - LM-White-Paper-Intel-Driven-Defense.pdf

File Edit Search View Format Scripts Templates Tools Window Help

Workspace

Open Files

Current: Desktop\LM-White-Paper-Intel-Driven-Defense.pdf

Documents\...\010 Templates\PDFTemplate.bt

Favorite Files

Recent Files

Bookmarked Files

Files Explorer

Inspector - PDFTemplate.bt

Name	Value	Start
struct PDFHeader sPDFHeader		0h
struct PDFComment sPDFComment		9h
struct PDFObj sPDFObj[0]	257 0 obj <</L...	10h
struct PDFObj sPDFObj[1]	278 0 obj <</S...	11h
struct PDFUnknown sPDFUnknown		1E7h
struct PDFTrailer sPDFTrailer		1F5h
struct PDFWhitespace sPDFWhitespace		1FC1h
struct PDFObj sPDFObj[2]	307 0 obj <</F...	20Dh
struct PDFObj sPDFObj[3]	258 0 obj <</...	360h
struct PDFObj sPDFObj[4]	259 0 obj <</C... 3A2h	3A2h
struct PDFObj sPDFObj[5]	260 0 obj <</F... 46Fh	46Fh
struct PDFObj sPDFObj[6]	261 0 obj <</F... F1Fh	F1Fh
struct PDFObj sPDFObj[7]	262 0 obj <</F... 46EAh	46EAh
struct PDFObj sPDFObj[8]	263 0 obj <</F... 4946h	4946h
struct PDFObj sPDFObj[9]	264 0 obj <</F... 48AAh	48AAh
struct PDFObj sPDFObj[10]	265 0 obj <</F... 4DF6h	4DF6h
struct PDFObj sPDFObj[11]	266 0 obj <</F... A924h	A924h
struct PDFObj sPDFObj[12]	267 0 obj <</F... E940h	E940h
struct PDFObj sPDFObj[13]	268 0 obj <</F... EB5Eh	EB5Eh
struct PDFObj sPDFObj[14]	269 0 obj <</F... EE7Ah	EE7Ah
struct PDFObj sPDFObj[15]	270 0 obj <</F... F07h	F07h
struct PDFObj sPDFObj[16]	271 0 obj <</F... F377h	F377h
struct PDFObj sPDFObj[17]	272 0 obj <</F... F532h	F532h
struct PDFObj sPDFObj[18]	273 0 obj <</F... 12459h	12459h
struct PDFObj sPDFObj[19]	274 0 obj <</F... 14B32h	14B32h

Auto Variables Bookmarks Functions

Output

```
PDFObject = 185
PDFComment = 1
PDFTrailer = 0
PDFWhitespace = 1
PDFUnknown = 2
```

LM-White-Paper-Intel-Driven-Defense.pdf

0123456789ABCDEF

```
0030h: 34 39 39 2F 4F 20 32 35 39 2F 45 20 31 32 34 31 499/O 259/E 1241
0040h: 33 38 2F 4E 20 31 34 2F 54 20 31 31 39 37 36 39 38/H 14/T 119769
0050h: 33 2F 48 20 5B 20 35 32 35 20 33 33 39 5D 3E 3E 3/H [ 525 339]>>
0060h: 0D 65 6E 64 6F 62 6A 0D 20 20 20 20 20 20 20 20 .endobj.
0070h: 20 20 0D 0A 32 37 38 20 30 20 6F 62 6A 0D 3C 3C . 278 0 obj.<<
0080h: 2F 44 65 63 6F 64 65 50 61 72 6D 73 3C 3C 2F 43 /DecodeParms<</C
0090h: 6F 6C 75 6D 6E 73 20 35 2F 50 72 65 64 69 63 74 olums 5/Predict
00A0h: 6F 72 20 31 32 3E 3E 2F 46 69 6C 74 65 72 2F 46 or 12>>/Filter/F
00B0h: 6C 61 74 65 44 65 63 6F 64 65 2F 49 44 5B 3C 41 lateDecode/ID[<A
00C0h: 33 45 43 43 39 34 45 35 34 37 34 46 31 45 36 43 3ECC94E5474F1E6C
00D0h: 41 44 42 38 34 38 41 43 41 38 37 31 33 42 41 3E ADB848AC8713BA>
00E0h: 3C 32 38 39 45 31 32 33 32 46 45 44 41 44 33 34 <289E1232FEDAD34
00F0h: 35 42 32 41 32 44 41 36 38 42 42 31 31 34 37 38 5E2A2DA68BB11478
0100h: 45 3E 5D 2F 49 6E 64 65 78 43 32 35 37 20 35 31 25/1/Index[257 53
0110h: 5D 2F 49 6E 66 6F 20 32 35 36 20 30 20 52 2F 4C /Info 256 0 R/L
0120h: 65 6E 67 74 68 20 31 30 37 2F 50 72 65 76 20 31 length 107/Prev 4
0130h: 33 30 31 36 30 34 33 63 65 6F 74 30 33 36 38 30 132594/Prev 358
```

Template Results - PDFTemplate.bt

Name	Value	Start	Size	Color	Comment
struct PDFHeader sPDFHeader		0h	9h	Fg: Bg:	
struct PDFComment sPDFComment		9h	7h	Fg: Bg:	
struct PDFObj sPDFObj[0]	257 0 obj <</L...	10h	64h	Fg: Bg:	
struct PDFObj sPDFObj[1]	278 0 obj <</S...	11h	74h	Fg: Bg:	
struct PDFUnknown sPDFUnknown		1E7h	1h	Fg: Bg:	
struct PDFTrailer sPDFTrailer		1F5h	7h	Fg: Bg:	
struct PDFWhitespace sPDFWhitespace		1FC1h	11h	Fg: Bg:	
struct PDFObj sPDFObj[2]	307 0 obj <</F...	20Dh	163h	Fg: Bg:	
struct PDFObj sPDFObj[3]	258 0 obj <</...	360h	42h	Fg: Bg:	
struct PDFObj sPDFObj[4]	259 0 obj <</C... 3A2h	3A2h	CDh	Fg: Bg:	
struct PDFObj sPDFObj[5]	260 0 obj <</F... 46Fh	46Fh	AD0h	Fg: Bg:	
struct PDFObj sPDFObj[6]	261 0 obj <</F... F1Fh	F1Fh	37C8h	Fg: Bg:	
struct PDFObj sPDFObj[7]	262 0 obj <</F... 46EAh	46EAh	26C4h	Fg: Bg:	
struct PDFObj sPDFObj[8]	263 0 obj <</F... 4946h	4946h	264Ch	Fg: Bg:	
struct PDFObj sPDFObj[9]	264 0 obj <</F... 48AAh	48AAh	24Ch	Fg: Bg:	
struct PDFObj sPDFObj[10]	265 0 obj <</F... 4DF6h	4DF6h	5F34h	Fg: Bg:	
struct PDFObj sPDFObj[11]	266 0 obj <</F... A924h	A924h	3C16h	Fg: Bg:	
struct PDFObj sPDFObj[12]	267 0 obj <</F... E940h	E940h	2A5h	Fg: Bg:	
struct PDFObj sPDFObj[13]	268 0 obj <</F... EB5Eh	EB5Eh	20Ch	Fg: Bg:	

恶意软件分析报告

□ 关键信息

■ 样本基本信息

样本编号	样本名称	样本生成（或编译）日期	样本类型	文件大小	样本 hash	样本描述

恶意软件分析报告

□ 关键信息

■ 样本基本信息

■ 样本行为信息

行为描述	属性	详细信息	备注
创建自启动项	修改注册表	路径: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run] 键: <u>Mytools</u> 类型: REG_SZ 值: "C:\Users\test\Documents\Shuame\Skd8821.exe"	
代码注入	修改进程内存	进程"Test.exe"(pid为 6916)通过 <u>OpenProecess</u> 、 <u>WriteProcessMemory</u> 函数向进程"explorer" (pid为 1108) 的内存写入数据。	

恶意软件样本分析实例

□ 样本分析实例

- 目的：熟悉一般分析流程和常用工具

- 步骤

- 在线分析和检测平台，获取样本的基本行为信息
 - 对关键模块进行静态分析
 - 对关键模块进行动态调试
 - 总结、完成报告
-