XDef 2012
对话·交流·合作

木马雪崩到APT的关联与必然

——对一次演讲的反思

江海客（肖新光）
安天实验室

演讲者简介

- 江海客，真名肖新光，ID：seak
- 安天实验室Founder之一，首席技术架构师
- AV老兵，不务正业偷艺7年（1993～2000），一心创业卖艺12年（2000～2012），为AV卖命不卖肾。

温故.2006

这是一个充满预言、谶语和诅咒的年代，这是一个人人皆神、诸佛具死的年代，我自己则每每常因某个只言片语的应验，找到先知先觉的感觉，但某一天我突然想到，我们过去登坛说法的话能否逐条用现实检验。

2006.9.25

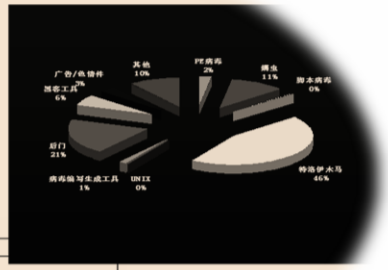
- 蠕虫时代的高潮已经落幕
- 木马开始呈现数量的爆炸式增长
- 2006年9月25日（疑似），武汉大学，笔者的一次汇报《后“冷战”时代的病毒捕获体制》
- 报告关键词：木马、蜜罐、旁路捕获、未知检测….
- 报告观点：当前木马与AV之间的对抗已经从辨识对抗、查杀对抗进入到体系对抗，笔者称之为后“冷战”时代。

2006.分析

对话·交流·合作

数量规模失控化

2004年，安天实验室平均每天接到6523次文件上报，共向病毒库中添加了200,047个新的独立病毒名称（含变种），其中木马类（木马、后门、黑客工具、广告色情件占绝大多数，部分蠕虫也具备木马性质）。而从1986年到2003年病毒数量的总和只有6万种。



2004 年各类病毒的产生数量如下：

PE 病毒	478
UNIX/Linux 系统病毒	33
蠕虫	2239
脚本病毒	81
特洛伊木马	8969
后门	4010
黑客工具	1241
广告/色情件	668
其他	2049

根据媒体报道，国有2200个站点创木马。根构统计

黑客技术泛

- 溢出技术：条件溢出木马
- 驱动技术：rootkit
- 流文件技术：无载体文件
- 信息伪装技术：非可执行格式

传统技术的主要挑战总结

- 数量失控
- 黑客技术
- 伪装技术
- 专有性
- 全面分析响应的工作量趋向不收敛
- 无法对抗各种非常规态木马
- 木马可复用性大大提高
- 采集工作异常困难

2006.预言

结论：木马动摇了AV根基

- 传统AV技术的根本链路是，编制>>流行>>捕获>>处理，捕获是AV的根基！！
- AV机理：以样本满足一定的流行范围或公开发布为基础，立足于后发式的一对一处理。
- 全面捕获已经趋近不可能，分析处理强度也趋向不收敛，必须有全新的思路作[illegible]。

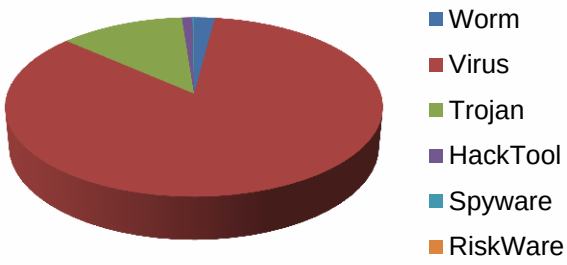
2005年，安天内部分析报告甚至给出了“中国信息安全将崩盘”于木马的结论。

迷失.2012

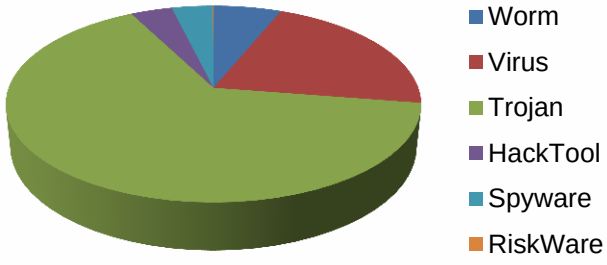
2012，一个让思想者茫然，行动者迷失的年份。

2000～2012数据回朔

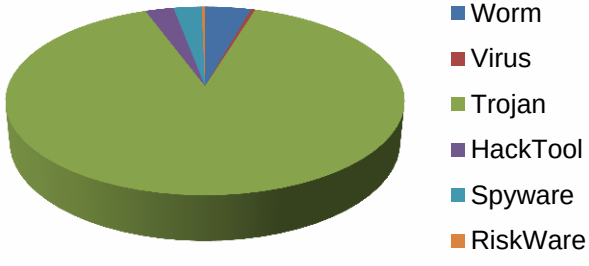
2000-10-24



2006-11-10



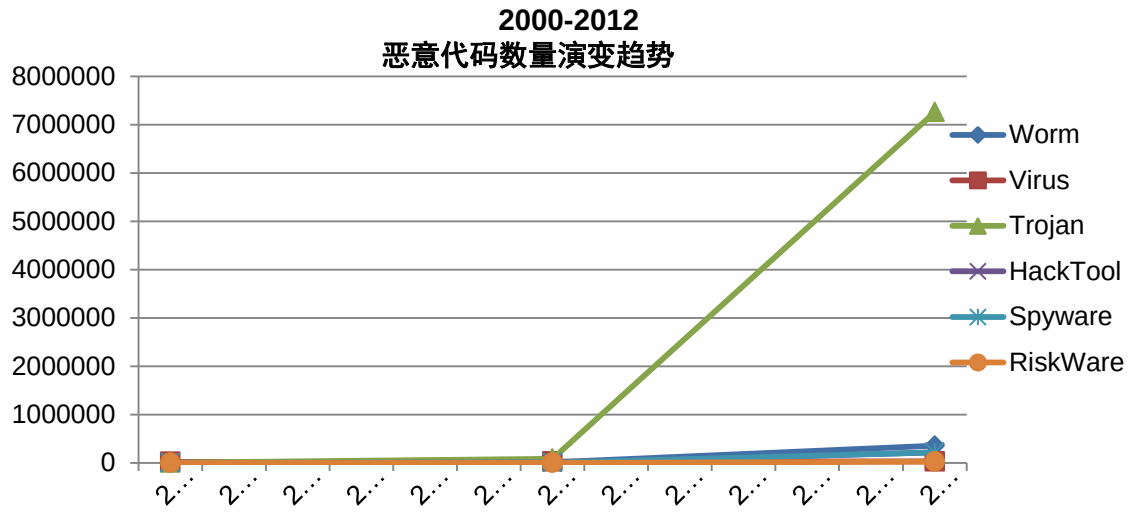
2012-11-27



日期/分类	2000/10/24	2006/11/10	2012/11/27
Worm	512	8109	354049
Virus	21006	27760	29940
Trojan	3066	84811	7262094
HackTool	260	4968	217502
Spyware	37	4899	214570
RiskWare	0	88	25800

来源：Kapersky对应日期病毒名列表

2006的结论应验了么？



- 木马数量爆炸增长没有能够遏制是真实的
- 但是：
  - 信息安全的崩盘了么？
  - AV根基动摇了么？
- 结论是——没有！

今天的威胁是什么？

APT(Advanced Persistent Threat)

Flame | Duqu | Gauss | Stuxnet

他们是木马么？是蠕虫么？是僵尸网络么？
都不是：他们是**APT**
我们最大的失误并不是没有很好遏制昨天的威胁，
而是没有应对今天的威胁

2006.我们预言了APT么？

专有化

- 经济利益化/政治利益化促进木马向定向性、专有化发展。
- 从传统的散步行为向定向行为转化，不需要大面积传播也能达到一定目的。

- 型有实无：APT不是一种木马！
- APT也不是一种新的恶意代码！
- APT的度量衡是什么？

2006.数据度量

对话·交流·合作

	个数	NAV	Panda	Pccillin	MCAFEE	KAV	
Wildlist	156	137	148	154	155	154/154	61
Supplemetal	113	97	101	107	112	106/108	38
	4	4	4/4	4	3	4	1
		238	253	265	270		

2001年Popsoft测试表明主流反病毒软件检出率都较高

	个数	江民KV	瑞星	金山	Pc-cillin	诺顿
bot	46	34	31	40	41	40
病毒	21	21	18	17	19	21
黑客工具	39	27	26	27	14	14
间谍软件	6	4	5	3	1	3
木马	281	179	212	206	153	206
蠕虫	31	28	28	28	28	30

2005年《CHIP》测试表明反病毒软件对木马检出率显著下降

2006年，我们用2005、2001两次的是的检出率对比作为度量衡得出恶意代码进入“新冷战”时代的结论，那么今天我们的度量衡又是什么？

攻守的不平衡

病毒名称	释放时间	发现时间
CodeRedII	2001年8月3日	2001年8月3日
冲击波(Blaster)	2003年8月11日	2003年8月12日
震荡波(Sasser)	2004年4月30日	2004年5月1日
Zotob	2005年8月13日	2005年8月16日
Nyxem	2006年1月20	2006年2月3日

在蠕虫时代，影响巨大的恶意代码捕获时间以小时和天为单位

病毒名称	释放时间	发现时间
Stuxnet	2009年6月	2010年7月
Duqu	2007年或2008年？	2011年8月
Flame	2007年12月之前？	2012年5月

在APT时代，对相关恶意代码的感知时间以年计算

境内外能力与信息的不对称

对话·交流·合作

时间阶段	时间	事件
	2010.06.17	Virusblokada上报样本
	2010.07.13	Symantec检测样本为W32.Temphid
	2010.07.15	Kaspersky三篇博文讨论LNK漏洞和签名驱动
	2010.07.15	安天捕获第一个样本，并添加检测规则。
①	2010.07.16	微软发布LNK漏洞预警
	2010.07.16	Symantec博文介绍Stuxnet基本情况
	2010.07.19	Kaspersky博文介绍LNK漏洞原理
	2010.07.20	Symantec检测到C&C流量
	2010.07.20	Kaspersky博文介绍Stuxnet的证书，
	2010.07.20	Symantec博文介绍Stuxnet传播方法
	2010.07.19	西门子报告Stuxnet攻击其SCADA系统
	2010.07.23	Kaspersky发表系列博文Myrtus and Guava的第四篇和第五篇，开始研究工控系统
	2010.08.06	Symantec发布博文称其是第一个针对工控系统的rootkit
	2010.08.18	安天发布一篇样本分析报告
②	2010.09.21	Symantec发表博文介绍Stuxnet感染PLC的过程
	2010.09.26	Kaspersky发布系列博文Myrtus and Guava，介绍与伊朗的关系
	2010.09.26	Symantec发布博文，介绍Stuxnet感染Step7工程的方法
	2010.09.27	安天发布第一版大报告。
	2010.09.30	Symantec在VB大会上演示PLC系统
	2010.10.11	安天补充了一篇后续报告。
③	2010.11.16	Symantec发布博文，称Stuxnet的攻击目标是伊朗某核电站中铀的浓缩设施
	2011.02	Kaspersky公布对Stuxnet时间戳的关联分析
	2011.12.28	Kaspersky公布Stuxnet与Duqu的关联分析
④	2012.01.23	安天完成关于WINCC对铀浓缩具体影响的有关分析。
	2012.01.23	安天完成Suxnet与Duqu的同源性分析并发布报告

国内厂商的分析明显比境外主流厂商迟缓，这是意识、投入等因素造成。但同时也是境内企业无法第一时间获得更多有效信息造成的。

弯路. 2006～2012

误判不是无代价的，误判必然导致错误的导向和行动。分析我们没有有效应对木马时代的原因，或许可以为我们没有如何应对APT时代提供参考。

向左转：蜜罐还是终端

2006，安天基于ARM设备的“蜜池”。

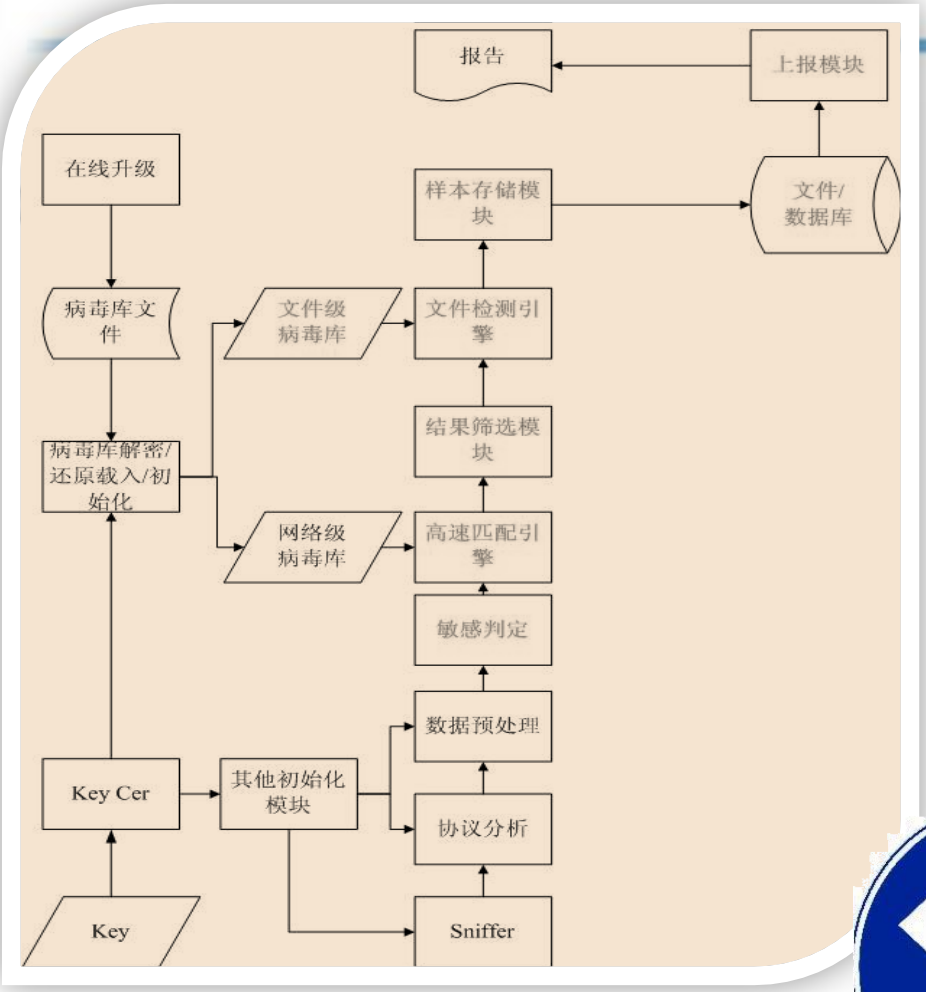
终端就是最好的蜜罐！

向左转：更敏感还是云

2006.未知检测：
提高启发式的敏感性
采用报警和上传不同的策略

云查杀：
对可执行对象无条件的上报

向左转：还原还是爬虫



基于爬虫的恶意资源获取

2006.基于旁路的还原捕获

还有还有

- 人工还是自动化？
- 静态还是动态 ？
- 改善脱壳和预处理还是改善捕获？
- …….
- 我们最初都选择了向左转（前者）！

弯路的分析

- AVER的传统局限性
  - 贫瘠资源局限了想象力
  - 狭义道德感局限了策略
  - 传统的惯性局限了方法

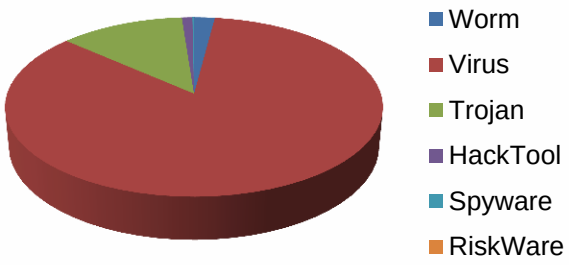
- 如何避免下一个误判？

思索.2012～201？

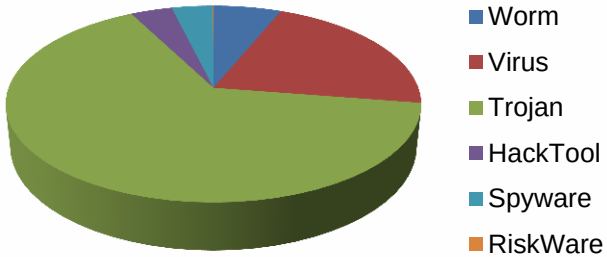
信息安全没有崩盘的原因，是因为应用跑得更快；
应用跑的令人心惊的原因，是应用忘记了带上安全伴跑。
向前走并没有错，我们只是没有绕过路上的石头！
但我们不能因为会绊倒石头拒绝向前！

2000～2012的演化原因

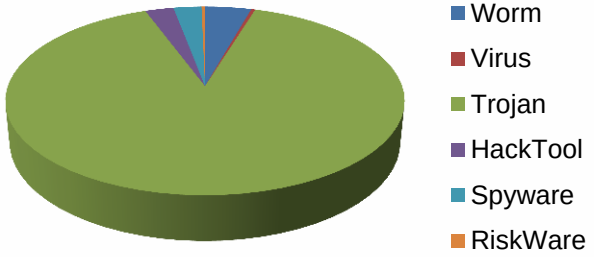
2000-10-24



2006-11-10

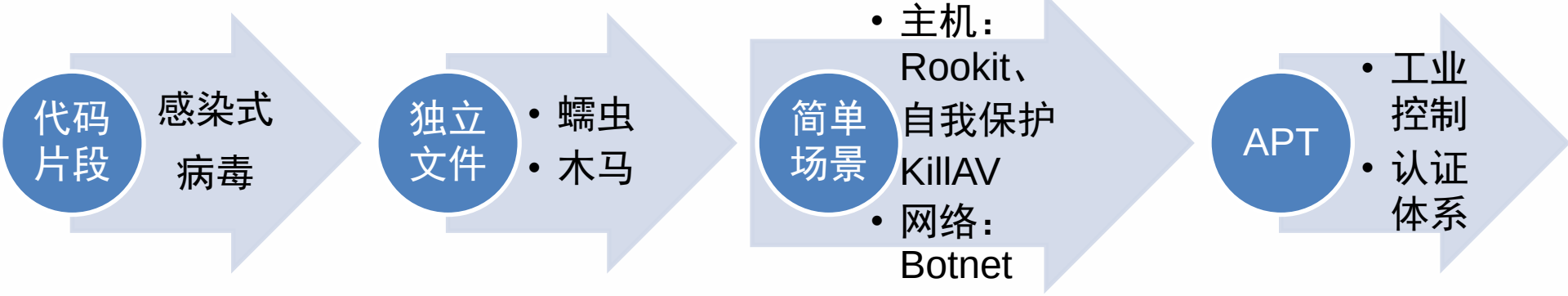


2012-11-27



日期/分类	2000/10/24	2006/11/10	2012/11/27
Worm	512	8109	354049
Virus	21006	27760	29940
Trojan	3066	84811	7262094
HackTool	260	4968	217502
Spyware	37	4899	214570
RiskWare	0	88	25800

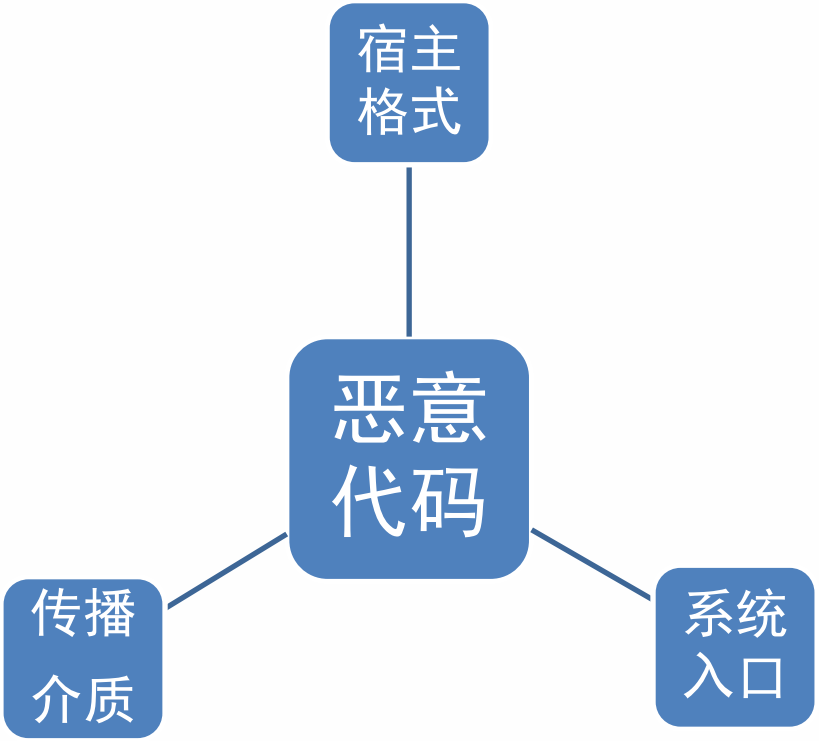
回顾过程演进


代码片段
感染式病毒
独立文件
• 蠕虫
• 木马
简单场景
• 主机：Rookit、自我保护KillAV
• 网络：Botnet
APT
• 工业控制
• 认证体系

插播-故事

我们习惯了观察沙子	• AV 的个体处理模式（第二次跌倒）
我们被沙子迷住了眼睛，因此没有发现飞来石头	• 我们对木马数量的恐惧
我们没有想到他（她）敢扔石头	• 我们没有想到大玩家入场

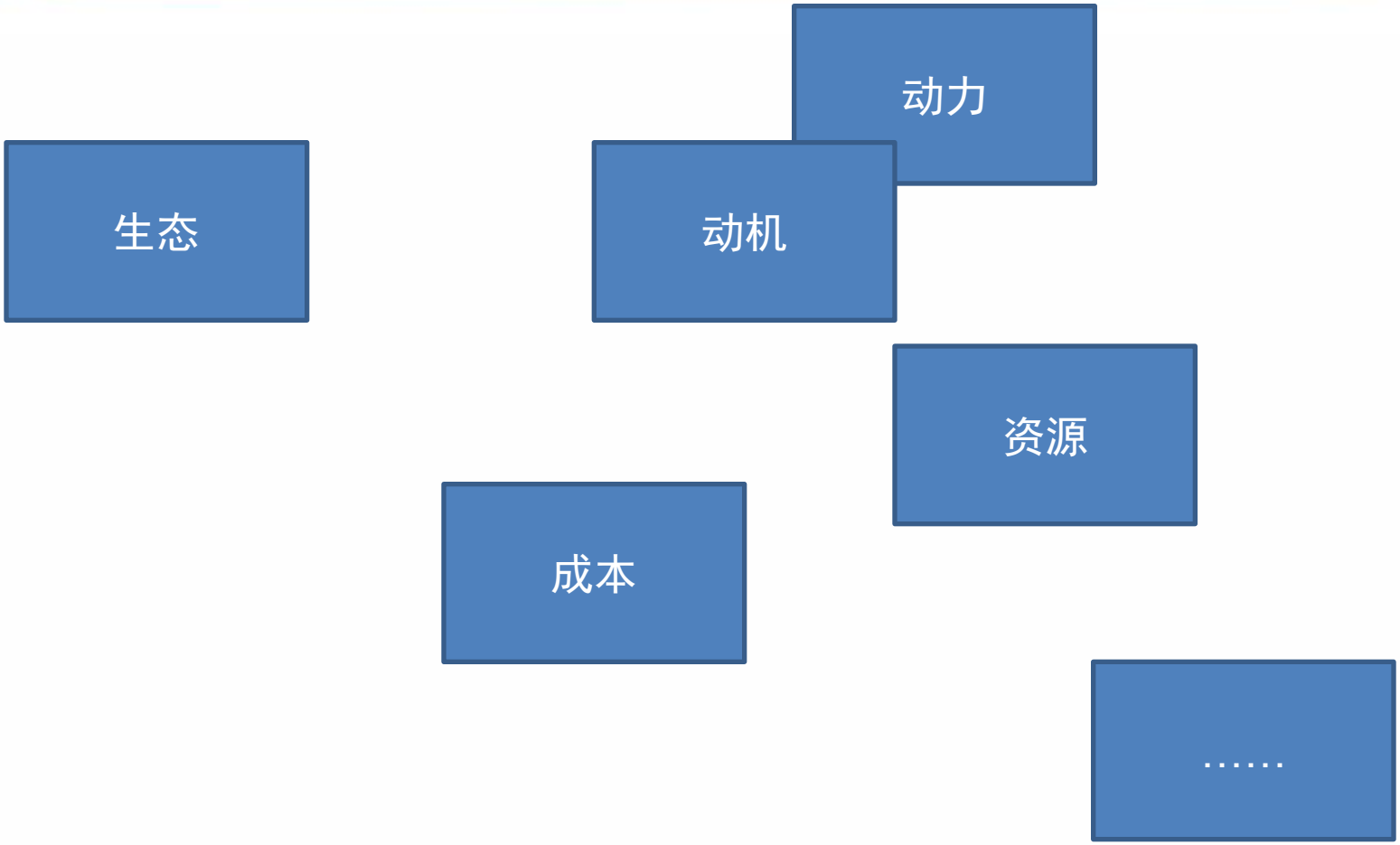
寻找新威胁要素



传统恶意代码威胁要素

新威胁要素是什么

关注新的关键词



有意思的对比

水木社区(展开完整界面) → 病毒讨论 → 精华区文章阅读

Virus 版 (精华区)

发信人: seak (江海客-加强计划性，开发无不胜), 信区: Virus
标　题: Red Code 2特急警报
发信站: BBS 水木清华站 (Mon Aug　6 23:50:01 2001)

Red Code 2特急警报
江海客(avbox@china.com)

自从昨晚到今天凌晨，我根据一些情况紧急贴出了Red Code的警报后，今天白天(8月6日)发现(特别是拿到样本并分析后)问题比我昨天想象的严重的多。

其严重问题包括：

1、当前在国内流行的病毒，虽然传播机理与Red Code相同，但是其危害要大的多，关键是所有感染了该变种蠕虫的机器，都等于被开设了两类及其危险的后门。应该说，国内目前有大量的NT/2000服务器，陷于极度危险的境地。千万恳请，国内有关单位和部门，不要掉以轻心，迅速检查你们的服务器，否则可能给国家或企业带来重大损失。

2、传播之广之快令人震惊，今天我们一台安装了单机IDS Numan NET的拨号节点，在不足10个小时，的连接时间中，收到了1034个Red Code蠕虫发出的请求。比昨天晚上继续增加。一些大系统的网络维护人员反映，有部分网段几乎瘫痪。

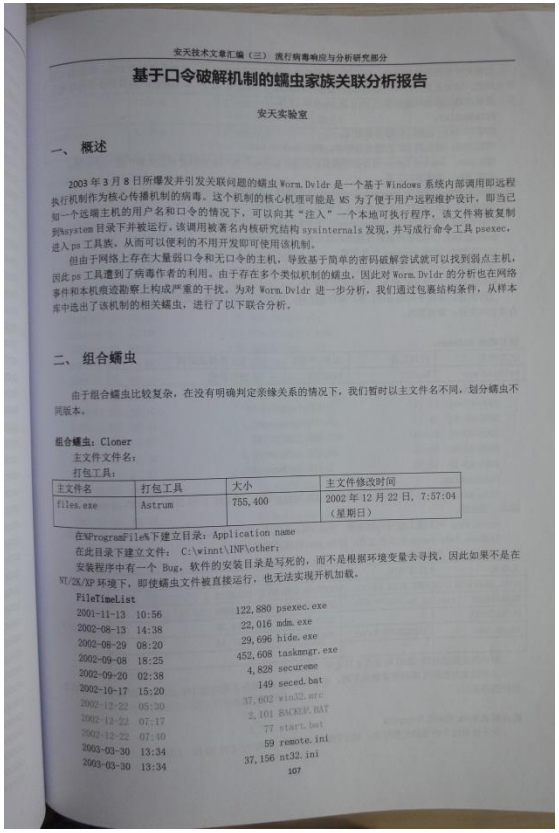
3、这个蠕虫从特性上看，有对Red Code的流行对中国进行报复的嫌疑，如果感染的系统不是中文平台，则用300个线程继续发出联接请求，如果是中文平台则用600个线程发出联接请求。因此中国和周边地区的传播比欧美会大大加快。

4、反病毒企业对该病毒的响应不是很快。由于Red Code2是没有文件载体的蠕虫，因此多数反病毒软件只能查出蠕虫拆离出的后门程序，但不能发现内存中的蠕虫本身。同时，普通用户除了这个后门程序，根本没有能力提取蠕虫的内存映像，我估计有部分反病毒企业目前还不明白事情的所以然。

5、一般用户不知如何修补自己的系统，使之不被感染。很多用户重装系统后再次遭受感染。Antiy Labs IDS开发组，紧急写了一个应急的查杀程序，授权病毒观察站virusview.net在相应的疫情相应栏目中发布。

下载地址为：

2001
红色代码预警
1页网帖



安天技术文章汇编（三） 流行病毒响应与分析研究部分

基于口令破解机制的蠕虫家族关联分析报告

安天实验室

一、 概述

2003 年 3 月 8 日所爆发并引发关联问题的蠕虫 Worm.Dvldr 是一个基于 Windows 系统内部调用即远程执行机制作为核心传播机制的病毒。这个机制的核心机理可能是 MS 为了便于用户远程维护设计，即当已知一个远端主机的用户名和口令的情况下，可以向其“注入”一个本地可执行程序，该文件将被复制到%system 目录下并被运行。该调用被著名内核研究结构 sysinternals 发现，并写成行命令工具 psexec，进入 ps 工具族。从而可以便利的不用开发即可使用该机制。

但由于网络上存在大量弱口令和无口令的主机，导致基于简单的密码破解尝试就可以找到弱点主机，因此 ps 工具遭到了病毒作者的利用。由于存在多个类似机制的蠕虫。因此对 Worm.Dvldr 的分析也在网络事件和本机痕迹勘察上构成严重的干扰。为对 Worm.Dvldr 进一步分析，我们通过包裹结构条件，从样本库中选出了该机制的相关蠕虫，进行了以下联合分析。

二、 组合蠕虫

由于组合蠕虫比较复杂，在没有明确判定亲缘关系的情况下，我们暂时以主文件名不同，划分蠕虫不同版本。

组合蠕虫：Cloner
主文件文件名：
打包工具：

主文件名	打包工具	大小	主文件修改时间
files.exe	Astrum	755,400	2002 年 12 月 22 日, 7:57:04 (星期日)

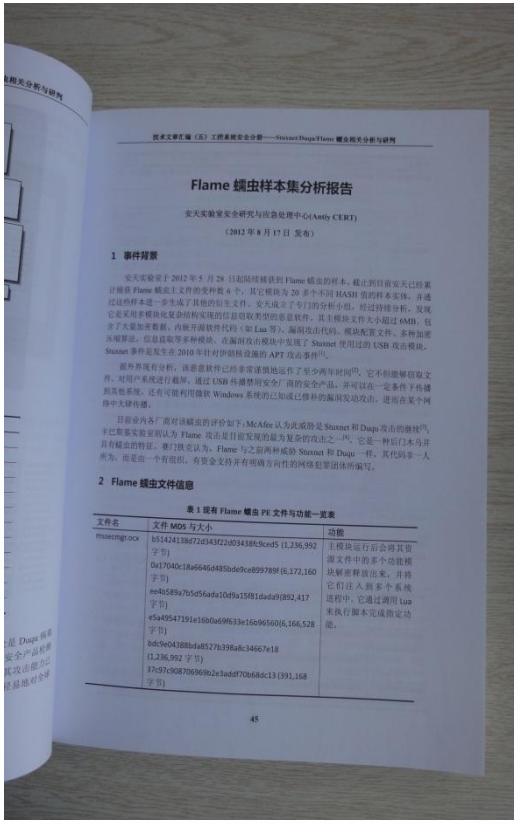
在%ProgramFile%下建立目录：Application name
在此目录下建立文件： C:\winnt\INF\other;
安装程序中有一个 Bug，软件的安装目录是写死的，而不是根据环境变量去寻找，因此如果不是在 NT/2K/XP 环境下，即使蠕虫文件被直接运行，也无法实现开机加载。

FileTimeList

2001-11-13	10:56	122,880 psexec.exe
2002-08-13	14:38	22,016 mdm.exe
2002-08-29	08:20	29,696 hide.exe
2002-09-08	18:25	452,608 taskmngr.exe
2002-09-20	02:38	4,828 secureme
2002-10-17	15:20	149 seced.bat
2002-12-22	05:30	37,602 win32.src
2002-12-22	07:17	2,101 BACKUP.BAT
2002-12-22	07:40	77 start.bat
2003-03-30	13:34	59 remote.ini
2003-03-30	13:34	37,156 nt32.ini

107

2003
口令蠕虫
13页分析报告



技术文章汇编（五）工控系统安全分析——Stuxnet/Duqu/Flame 蠕虫相关分析与研究

Flame 蠕虫样本集分析报告

安天实验室安全研究与应急处理中心(Antiy CERT)

（2012 年 8 月 17 日 发布）

1 事件背景

安天实验室于 2012 年 5 月 28 日起陆续接获到 Flame 蠕虫的样本，截止到目前安天已经累计捕获 Flame 蠕虫主文件的变种数 6 个，其它模块为 20 多个不同 HASH 值的样本实体。并通过这些样本进一步生成了其他的衍生文件。安天成立了专门的分析小组，经过持续分析，发现它是采用多模块化复杂结构实现的信息窃取类型的恶意软件。其主模块文件大小超过 6MB，包含了大量加密数据、内嵌开源软件代码（如 Lua 等）、漏洞攻击代码、模块配置文件。多种加密压缩算法，信息窃取等多种模块。在漏洞攻击模块中发现了 Stuxnet 使用过的 USB 攻击模块，Stuxnet 事件是发生在 2010 年针对伊朗核设施的 APT 攻击事件[1]。

一般外界现有分析，该恶意软件已经非常谨慎地运作了至少两年时间[2]，它不但能够窃取文件，对用户系统进行截屏，通过 USB 传播禁用安全厂商的安全产品，并可以在一定条件下传播到其他系统，还有可能利用微软 Windows 系统的已知或已修补的漏洞发动攻击，进而在某个网络中大肆传播。

2 Flame 蠕虫文件信息

表 1 现有 Flame 蠕虫 PE 文件与功能一览表

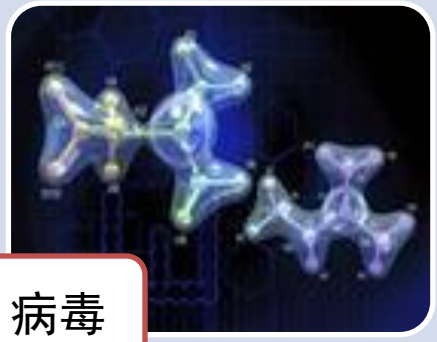
文件名	文件 MD5 与大小	功能
mssecmgr.ocx	b51424138d72d343f22d034385c9ced5 (1,236,992 字节)	主模块运行后会将其资源文件中的多个功能模块解密释放出来，并将它们注入到多个系统进程中。它通过调用 lua 来执行脚本完成指定功能。
	0a17040c18a6646d485de9ce899789f (6,172,160 字节)	
	ee4b589a7b5d56ada10d9a15881dada9 (892,417 字节)	
	e5a49547191e168b0a69f633e16b96560 (6,166,528 字节)	
	bdc9e04388bda8527b398a8c34667e18 (1,236,992 字节)	
	37c97c908709869b2e3addf70b68dc13 (391,168 字节)	

45

2012
Flame
92页分析报告

AVER工作方法的变迁

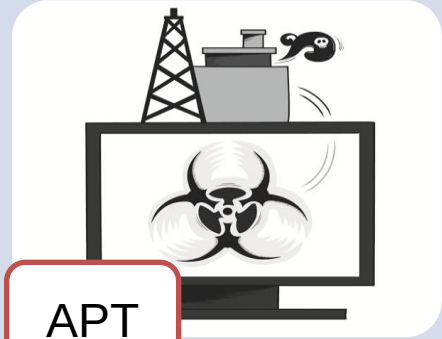
对话·交流·合作



病毒

蠕虫

木马



APT

完整性焦虑

- 人工分析
- 清除

及时性焦虑

- 发现
- 遏制

数量焦虑

- 自动分析
- 主动防御

后果焦虑

- 深度分析
- 回朔评估

尾声

- 比尔.盖茨说：“五年，这就是我们向前能看到最远的时间。”
- 我无法判断我能向前看多远，但可以肯定的是要比比尔.盖茨近得多。
- 但我们可以回头看……
- 我今天的每一句话，都比六年前，谨慎的多，因为我希望六年后，有勇气回顾今天的话。

谢谢各位专家老师和同学们

求点击：http://www.antiy.net

求批判：http://www.virusview.net

求关注：http://weibo.com/seak