ANTIY 安天 创造安全每一天

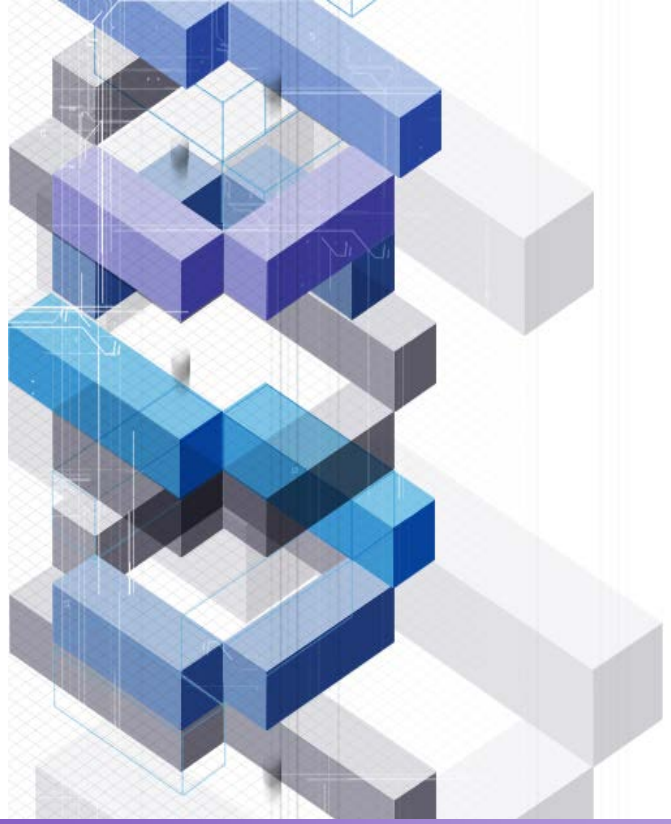
管中窥豹——Stuxnet、Duqu和Flame的分析碎片与反思

安天实验室

2012.6.15

说在前面

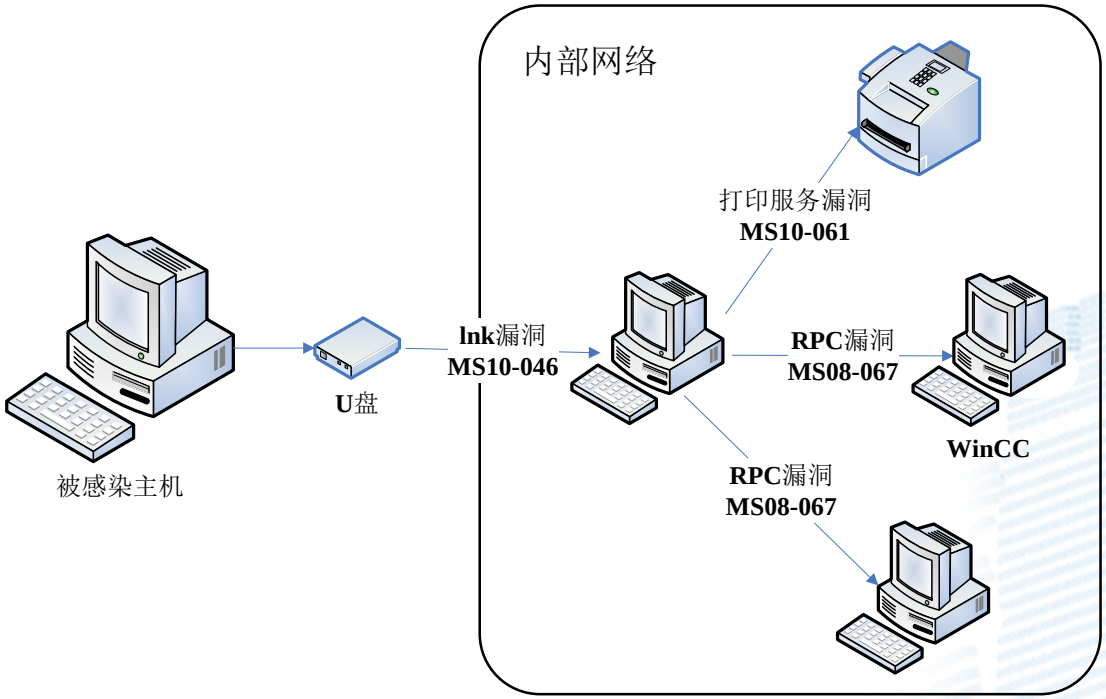

技术文章汇编（三）
专题报告分册
安天实验室
2011年6月
（安天内部资料 注意保存）
安天技术文章汇编（五）
工业控制系统安全分册
2011年7月26日
（安天内部资料 注意保存）
安天
技术文章汇编（六）
文献翻译分册
2011年3月
技术文章汇编（八）
移动安全分册



第一窥：一个行为的断链拼接

本章围绕安天分析中，遇到分析报告读者提出的三个问题，而展开。

一个都知道的故事


内部网络
打印服务漏洞
MS10-061
被感染主机
U盘
lnk漏洞
MS10-046
RPC漏洞
MS08-067
WinCC
RPC漏洞
MS08-067

为何不能复现U盘传播?

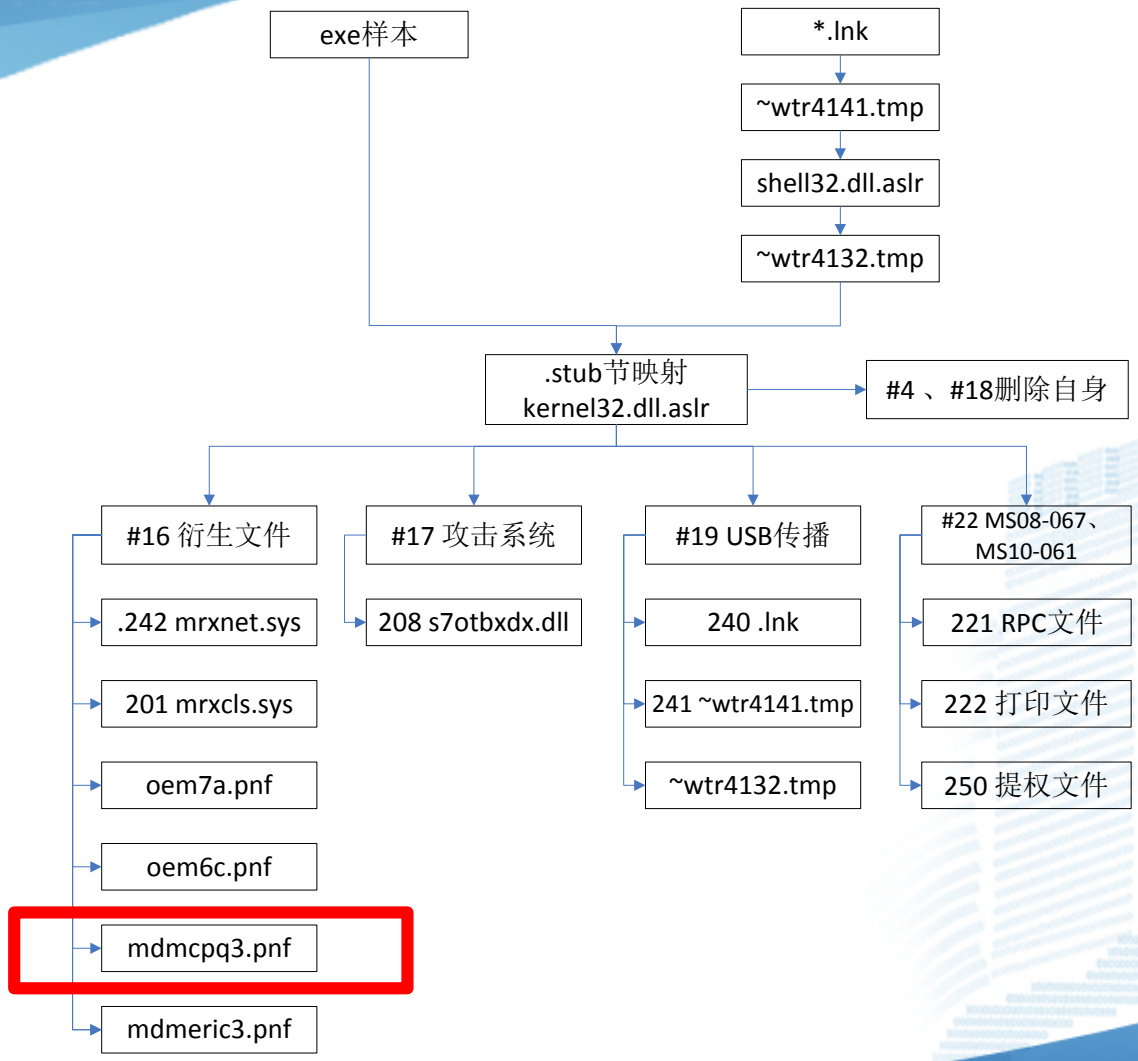
反汇编	文本字串
MOV EBX,Region00.10061B30	{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
PUSH Region00.10061A80	storage#volume#
MOV EDI,Region00.10061A0C	\\.\
MOV EBP,Region00.10061BCC	%s%s%s#%s
PUSH Region00.10061AA0	storage#volume#1&19f7e59c&0&
PUSH Region00.10061A4C	storage#removablemedia#8&
MOV EBP,Region00.10061BE0	%s%s%x&0&rm#%s
PUSH Region00.10061A18	storage#removablemedia#7&

查找U盘

反汇编	文本字串
PUSH Region00.100618A4	copy of shortcut to.lnk
PUSH Region00.100618D4	copy of
PUSH Region00.100618E8	~wtr4141.tmp
PUSH Region00.10061904	~wtr4132.tmp
PUSH Region00.1005CD1C	*
PUSH Region00.100618E8	~wtr4141.tmp
PUSH Region00.10061904	~wtr4132.tmp
PUSH Region00.1005CD20	global\wkssvcshutdownevent2
PUSH Region00.100618E8	~wtr4141.tmp
PUSH Region00.10061904	~wtr4132.tmp

拷贝文件到U盘

传播的关键


exe样本
*.lnk
~wtr4141.tmp
shell32.dll.aslr
~wtr4132.tmp
.stub节映射
kernel32.dll.aslr
#4 、#18删除自身
#16 衍生文件
.242 mrxnet.sys
201 mrxcls.sys
oem7a.pnf
oem6c.pnf
mdmcpq3.pnf
mdmeric3.pnf
#17 攻击系统
208 s7otbxdx.dll
#19 USB传播
240 .lnk
241 ~wtr4141.tmp
~wtr4132.tmp
#22 MS08-067、
MS10-061
221 RPC文件
222 打印文件
250 提权文件

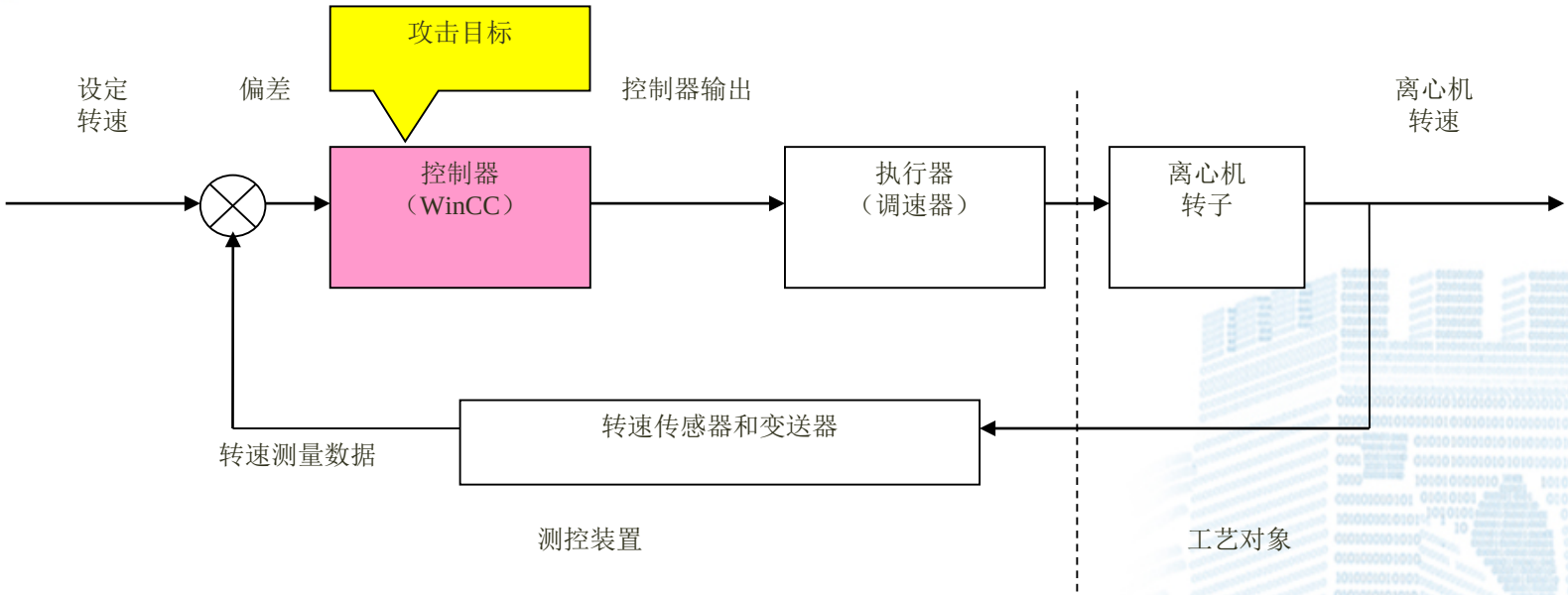
在何种条件下满足U盘传播？

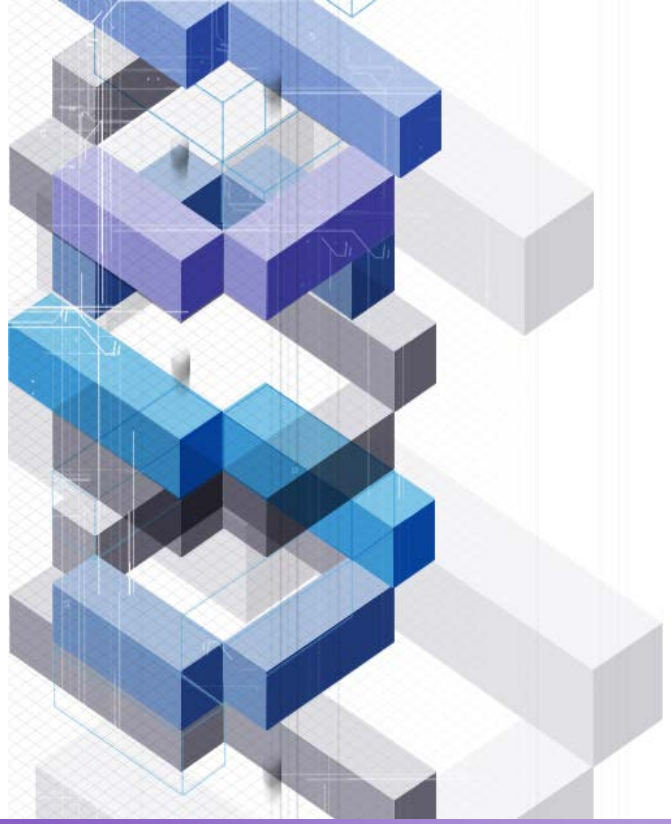
mdmcpq3.PNF

```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 09 05 79 AE 14 00 00 00 BF F1 71 D3 44 07 00 00 ; ..y?...狂q覾...
00000010h: 4C 04 00 00 03 00 00 00 01 00 00 00 02 00 00 00 ; L...............
00000020h: 08 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 ; ................
00000030h: E0 93 04 00 E0 70 72 00 80 84 1E 00 FE 04 00 00 ; 鄴..郠r.€?.?..
00000040h: 01 00 00 00 01 00 00 00 01 00 00 00 80 EE 36 00 ; ............€?.
00000050h: 64 00 00 00 2C 01 00 00 58 02 00 00 84 03 00 00 ; d...,...X...?..
00000060h: 50 46 00 00 08 52 00 00 01 00 00 00 00 00 00 00 ; PF...R.........
00000070h: 00 00 00 00 15 00 00 00 00 00 CB AA 7D A8 CB 01 ; ..........霜}了.
00000080h: 03 00 00 00 40 4B 4C 00 03 00 00 00 00 C0 45 4C ; ....@KL......繷L
00000090h: 9C 51 CD 01 38 31 00 00 00 00 00 00 00 00 00 00 ; 淨?81..........
000000a0h: 00 00 00 00 04 F2 CB 1C 60 5D CB 01 01 00 00 00 ; .....蜜.`]?....
000000b0h: 00 00 00 00 04 F2 CB 1C 60 5D CB 01 00 00 00 00 ; .....蜜.`]?....
000000c0h: 5A 00 00 00 87 00 00 00 01 00 00 00 77 00 77 00 ; Z...?.....w.w.
000000d0h: 77 00 2E 00 77 00 69 00 6E 00 64 00 6F 00 77 00 ; w...w.i.n.d.o.w.
000000e0h: 73 00 75 00 70 00 64 00 61 00 74 00 65 00 2E 00 ; s.u.p.d.a.t.e...
000000f0h: 63 00 6F 00 6D 00 00 00 00 00 00 00 00 00 00 00 ; c.o.m...........
00000100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000110h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000120h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000130h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000140h: 00 00 00 00 00 00 00 00 00 00 00 00 77 00 77 00 ; ............w.w.
00000150h: 77 00 2E 00 6D 00 73 00 6E 00 2E 00 63 00 6F 00 ; w...m.s.n...c.o.
00000160h: 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; m...............
00000170h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000180h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000001c0h: 00 00 00 00 00 00 00 00 00 00 00 00 77 00 77 00 ; ............w.w.
000001d0h: 77 00 2E 00 6D 00 79 00 70 00 72 00 65 00 6D 00 ; w...m.y.p.r.e.m.
000001e0h: 69 00 65 00 72 00 66 00 75 00 74 00 62 00 6F 00 ; i.e.r.f.u.t.b.o.
000001f0h: 6C 00 2E 00 63 00 6F 00 6D 00 00 00 00 00 00 00 ; l...c.o.m.......
00000200h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000230h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000240h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 69 00 ; ............i.n.
00000250h: 64 00 65 00 78 00 2E 00 70 00 68 00 70 00 3F 00 ; d.e.x...p.h.p.?.
00000260h: 64 00 61 00 74 00 61 00 00 00 00 00 00 00 00 00 ; d.a.t.a.........
00000270h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000280h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000290h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000002a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000002b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

偏移0x6c、0x70、0xc8处的标记位
偏移0x78、0x7c处的时间戳
偏移0x80、0x84处的数值

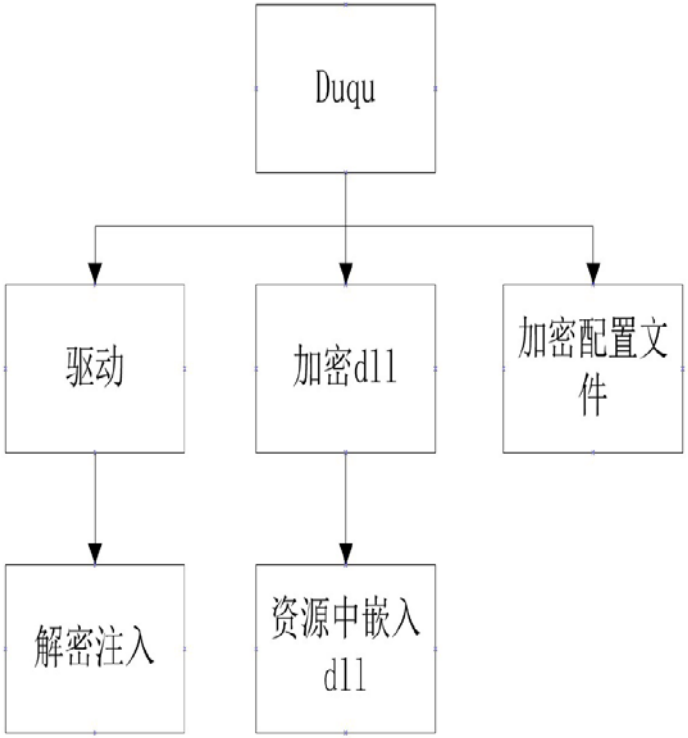
WinCC之后发生了什么？

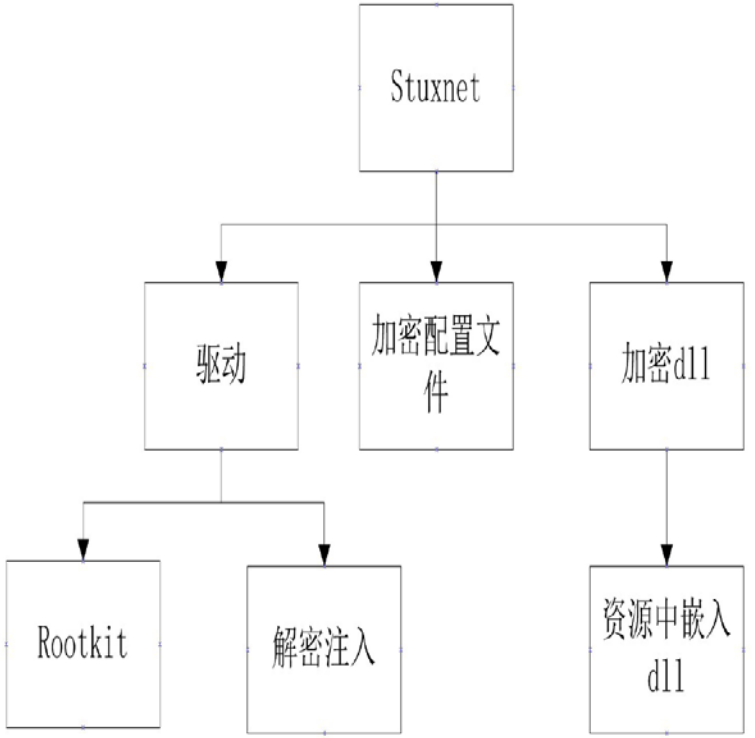




第二窥：同源性分析

Stuxnet与Duqu的结构





结构和方法的相似并不能证明具有关联

哪些才是关键比较点？

功能	Stuxnet	Duqu
模块化组件	✓	✓
内核rootkit	✓	✓ 非常相似
驱动数字证书	Realtek, JMicron	C-Media
注入进程A/V列表	✓	✓ 基于 Stuxnet.
3 个加密配置文件	✓	✓ 几乎完全一样
键盘记录模块	Duqu ☺	✓
PLC 功能模块	✓	× 不同于stuxnet
通过本地共享感染	✓	✓
利用0-day	✓	0-day, win32k.sys
资源文件释放dll	✓ (多个)	✓ (一个)
RPC 通信	✓	✓
Port 80/443	?（80）	✓ 相似
指定魔法数字	✓	✓ I
错误处理	✓	✓

关键判据：代码片段

```
mov     eax, dword ptr byte_15190
test    al, 1
jz      short loc_10611
mov     ecx, ds:InitSafeBootMode
cmp     dword ptr [ecx], 0
jz      short loc_10611
mov     eax, 0C0000001h
jmp     short loc_10632
-------------------------------------------------------

                        ; CODE XREF: DriverEntry+8D↑j
                        ; DriverEntry+98↑j
mov     edx, dword ptr byte_15190
test    edx, 2
jz      short loc_10630
mov     eax, ds:KdDebuggerEnabled
cmp     byte ptr [eax], 0
jz      short loc_10630
```

Duqu判定系统状态

```
mov     eax, dword_13E99
test    al, 1
jz      short loc_1044C
mov     eax, ds:InitSafeBootMode
cmp     [eax], ebx
jz      short loc_1044C

                        ; CODE XREF: DriverEntry+B2↓j
mov     eax, 0C0000001h
jmp     short loc_10460
-------------------------------------------------------

                        ; CODE XREF: DriverEntry+90↑j
                        ; DriverEntry+99↑j
mov     eax, dword_13E99
test    al, 2
jz      short loc_1045E
mov     eax, ds:KdDebuggerEnabled
cmp     [eax], bl
jnz     short loc_10445
```

Stuxnet判定系统状态

关键证据：数据相似

Duqu的注册表数据	Stuxnet的注册表数据

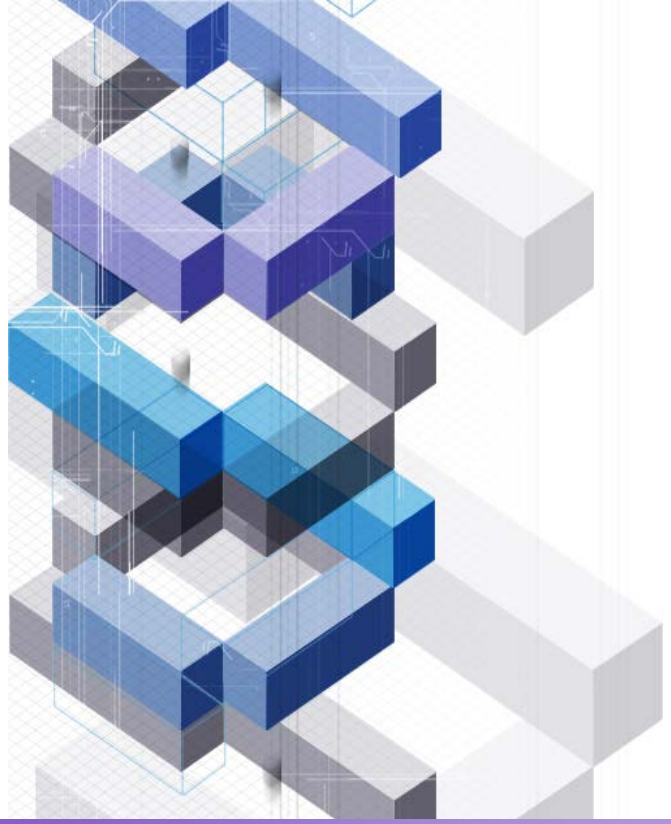
DWORD control[4]
DWORD encryption_key
DWORD sizeof_processname
BYTE processname[sizeof_processname]
DWORD sizeof_dllpath
BYTE dllpath[sizeof_dllpath]
	DWORD control[4]
	WORD expNumber; //注入dll调用的导出函数
	WORD Flags;
	DWORD encryption_key
	DWORD reserved ;
	//List
	DWORD sizeof_processname
	UNICODE processname[sizeof_processname]
	DWORD sizeof_dllpath
	UNICODE dllpath[sizeof_dllpath]

关键证据：共同的错误（获取XP操作系统版本）

```
                                ; CODE XREF: sub_12A00+5C↑j
push    ebx                     ; CSDVersion
push    ebx                     ; BuildNumber
lea     edx, [esp+140h+MajorVersion]
push    edx                     ; MinorVersion
lea     eax, [esp+144h+MinorVersion]
push    eax                     ; MajorVersion
mov     [esp+148h+MinorVersion], ebx
mov     [esp+148h+MajorVersion], ebx
call    esi ; PsGetVersion
cmp     [esp+138h+MinorVersion], 5
jnz     short loc_12A90
cmp     [esp+138h+MajorVersion], 1
jz      loc_12B10
```

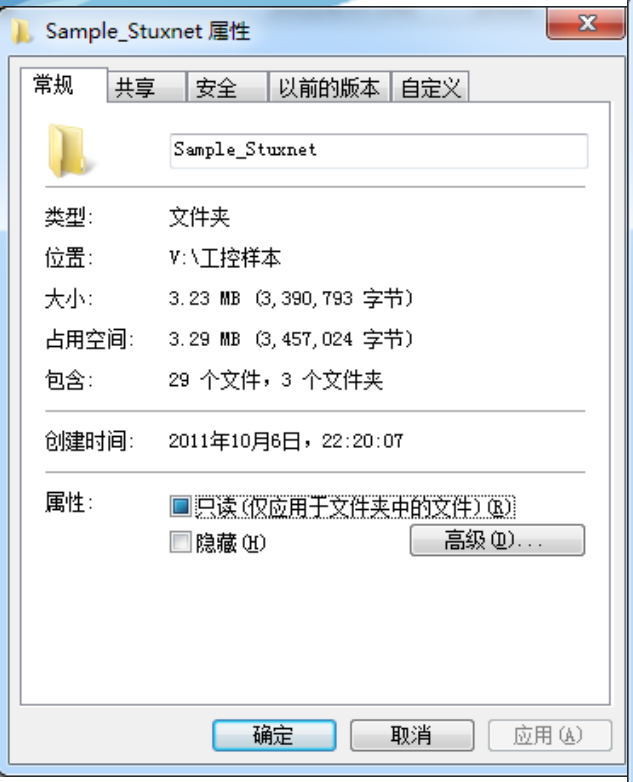
比较总结

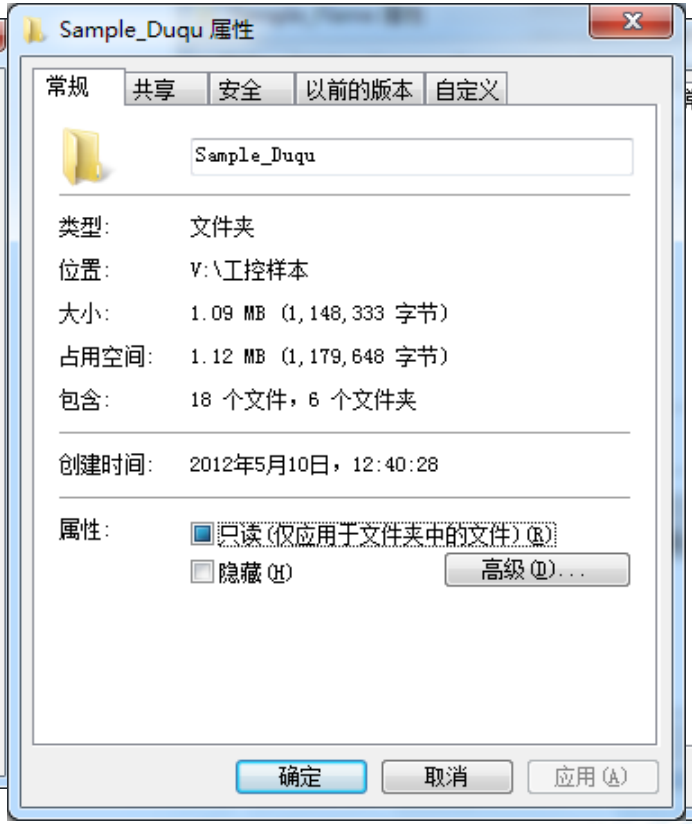
比较项目	Duqu木马	Stuxnet蠕虫
功能模块化	是	
Ring0注入方式	PsSetLoadImageNotifyRoutine	
Ring3注入方式	Hook ntdll.dll	
注入系统进程	是	
资源嵌入DLL模块	一个	多个
利用微软漏洞	是	
使用数字签名	是	
包括RPC通讯模块	是	
配置文件解密密钥	0xae240682	0x01ae0000
注册表解密密钥	0xae240682	
Magic number	0x90,0x05,0x79,0xae	
运行模式判断代码存在Bug	是	
注册表操作代码存在Bug	是	
攻击工业控制系统	否	是
驱动程序编译环境	Microsoft Visual C++ 6.0	Microsoft Visual C++ 7.0

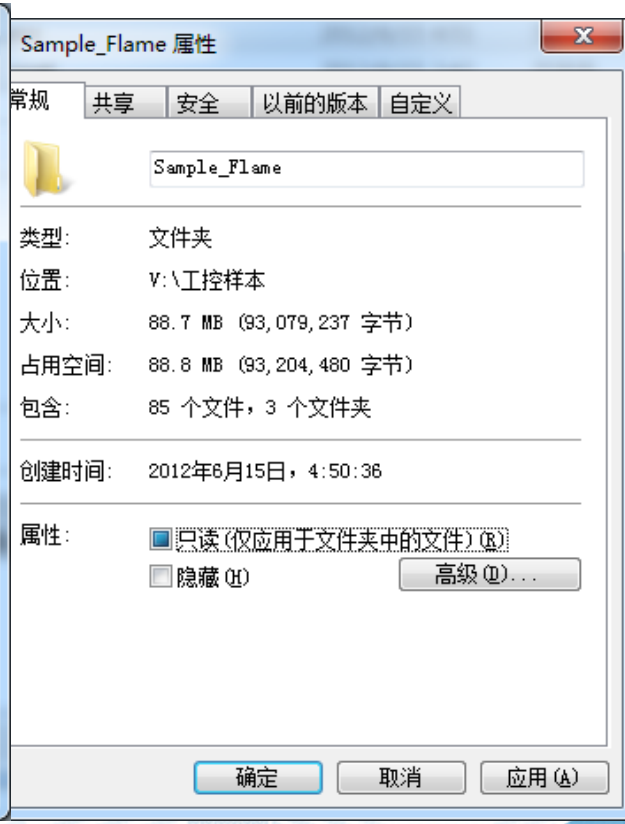


第三窥：无奈的渐进分析

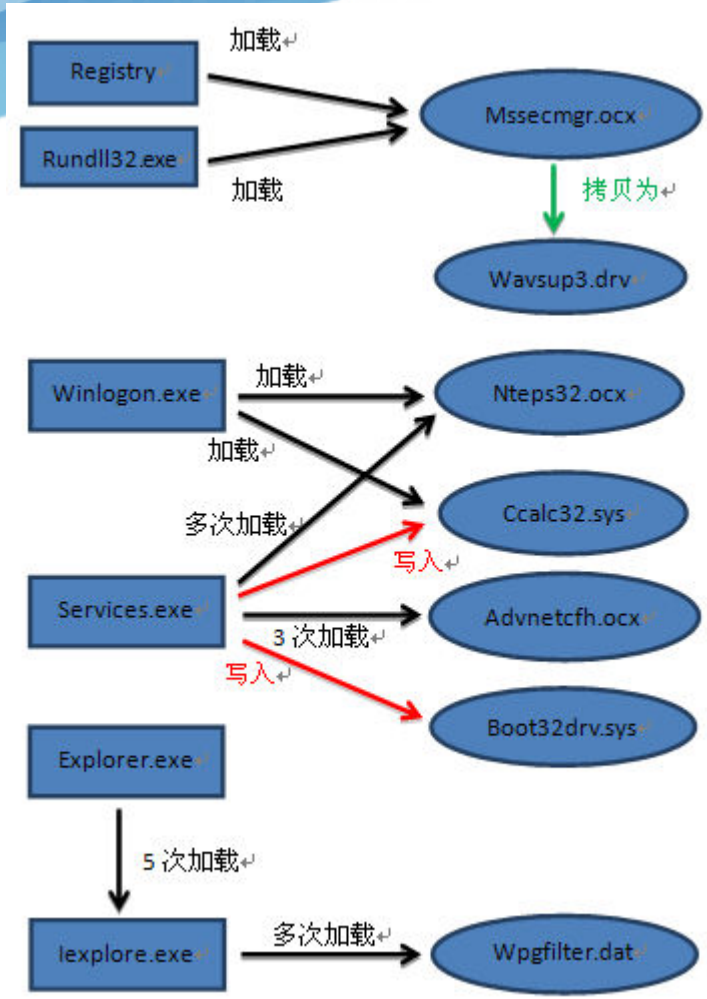
让我们看看这些样本


Sample_Stuxnet 属性
常规
共享
安全
以前的版本
自定义
Sample_Stuxnet
类型: 文件夹
位置: V:\工控样本
大小: 3.23 MB (3,390,793 字节)
占用空间: 3.29 MB (3,457,024 字节)
包含: 29 个文件，3 个文件夹
创建时间: 2011年10月6日，22:20:07
属性:
只读(仅应用于文件夹中的文件)(R)
隐藏(H)
高级(D)...
确定
取消
应用(A)

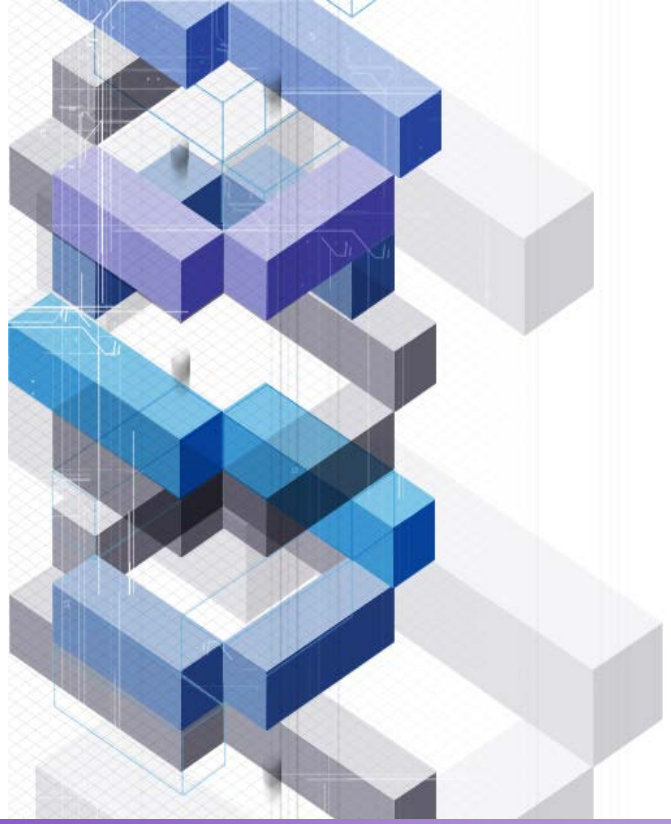

Sample_Duqu 属性
常规
共享
安全
以前的版本
自定义
Sample_Duqu
类型: 文件夹
位置: V:\工控样本
大小: 1.09 MB (1,148,333 字节)
占用空间: 1.12 MB (1,179,648 字节)
包含: 18 个文件，6 个文件夹
创建时间: 2012年5月10日，12:40:28
属性:
只读(仅应用于文件夹中的文件)(R)
隐藏(H)
高级(D)...
确定
取消
应用(A)


Sample_Flame 属性
常规
共享
安全
以前的版本
自定义
Sample_Flame
类型: 文件夹
位置: V:\工控样本
大小: 88.7 MB (93,079,237 字节)
占用空间: 88.8 MB (93,204,480 字节)
包含: 85 个文件，3 个文件夹
创建时间: 2012年6月15日，4:50:36
属性:
只读(仅应用于文件夹中的文件)(R)
隐藏(H)
高级(D)...
确定
取消
应用(A)

当分析变成不可能



Flame模块共有20MB大小，大部分模块都是函数库，用来处理SSL流量，SSH链接，嗅探，攻击和拦截通讯等。我们用了几个月的时间分析Stuxnet仅500K大小的文件，那么我们将需要几年的时间去完全明白Flame 20MB大小的文件。——卡巴斯基
《Flame病毒问答》



总结：重大样本的分析反思

工作汇总

文献题目	发布情况
Stuxnet木马分析报告	公开
对Stuxnet蠕虫攻击工业控制系统事件的综合报告（中英文版）	公开
对Stuxnet蠕虫的后续分析报告	公开
工业控制系统中的现场总线安全性	内部
Trojan-Win32.DuQu.a分析报告	公开
Duqu与Stuxnet：基于编码心理学的同源分析	公开
从Duqu病毒Stuxnet蠕虫的同源性看工业控制系统安全	内部
探索Duqu木马的身世之谜——Duqu和Stuxnet同源性分析	公开
对Flame病毒攻击事件的分析报告	公开
soapr32.ocx模块分析	公开
Nteps32.ocx的功能分析	公开
msglu32.ocx模块分析	公开

基于综合分析，编写各种文献16篇，
其中10篇已在网络/媒体上公开，2篇在安天内部发布，4篇为专项呈报。

Win32.Stuxnet蠕虫档案
使用SCADA木马攻击电网
Flamer：针对中东的非常复杂隐秘的威胁.
Flame病毒之问与答
Skywiper--网络之战的“火焰”

根据管理部门的需求，翻译文献5篇。

累计人工分析样本文件近百个
提取网络检测规则多条
编写专杀工具一个
制作工控系统安全威胁实景模拟系统一套

反思之一：人力投入

Kaspersky	Symantec	Antiy（安天）
Nicolas Falliere, 高级软件工程师 Liam O Murchu, 开发经理 Eric Chien, Symantec安全响应技术总监 Patrick Fitzgerald，高级工程师 Aniket Amdekar，高级工程师 Fergal Ladley，高级工程师	Alexander Gostev, 全球研发与分析部，首席安全专家 Roel Schouwenberg, 高级反病毒研究员 Costin Raiu, 全球研发与分析部，总监 Ryan Naraine，高级工程师 Roel Schouwenberg，高级工程师	GAo, 病毒分析组组长 Bughouse, 病毒分析工程师 Shuat, 病毒分析工程师 Skyriver, 病毒分析工程师 Tbsoft,高级电子工程师

人员层级？

人员构成？

人月投入？

反思之二：成果对比

		Kaspersky	Symantec	Antiy（安天）
博客与单点分析	数量	13	21	1
	首发时间	2010.07.15	2010.07.16	2010.08.18
	结束时间	2011.12.28	2011.07.11	N/A
	时间跨度	一年半	一年	N/A
正式报告	篇幅	7篇系列	69页	16页
	结束时间	N/A	2010.09.30	2010.09.27
	结束时间	N/A	2011.02.11	2010.09.30
	更新次数	N/A	4次	5次
公开演讲	首次时间	2010.09.30	2010.09.30	2011.04.28
	首次场景	VB2010	VB2010	部委汇报

反思之三：时间线分析

时间阶段	时间	事件
①	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。
	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
②	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
	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
④	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
	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

漏洞和证书

工控系统

具象目标

攻击朔源

特别感怀

安天面临的问题是国内厂商普遍问题。

面对大玩家入场，我们还没有做好准备。

人是在斗争中变得正确，
而不是等到正确了才去斗争。

谢谢各位专家领导