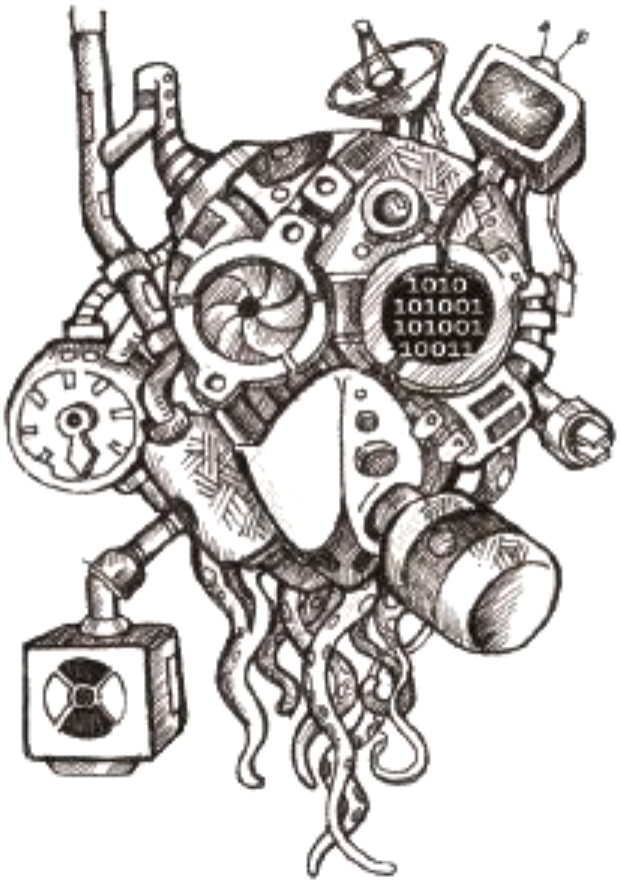
对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告

安天安全研究与应急处理中心(Antiy CERT)



首次发布时间：2010 年 9 月 27 日 21 时

本版本更新时间：2010 年 9 月 30 日 14 时

目 录

1 事件背景

近日，国内外多家媒体相继报道了 Stuxnet 蠕虫对西门子公司的数据采集与监控系统 SIMATIC WinCC 进行攻击的事件，称其为“超级病毒”、“超级工厂病毒”，并形容成“超级武器”、“潘多拉的魔盒”。

Stuxnet 蠕虫（俗称“震网”、“双子”）在今年 7 月开始爆发。它利用了微软操作系统中至少 4 个漏洞，其中有 3 个全新的零日漏洞；为衍生的驱动程序使用有效的数字签名；通过一套完整的入侵和传播流程，突破工业专用局域网的物理限制；利用 WinCC 系统的 2 个漏洞，对其展开攻击。它是第一个直接破坏现实世界中工业基础设施的恶意代码。据赛门铁克公司的统计，目前全球已有约 45000 个网络被该蠕虫感染，其中 60%的受害主机位于伊朗境内。伊朗政府已经确认该国的布什尔核电站遭到 Stuxnet 蠕虫的攻击。

安天实验室于 7 月 15 日捕获到 Stuxnet 蠕虫的第一个变种，在第一时间展开分析，发布了分析报告及防范措施，并对其持续跟踪。截止至本报告发布，安天已经累计捕获 13 个变种、 600 多个不同哈希值的样本实体。

2 样本典型行为分析

2.1 运行环境

Stuxnet 蠕虫在下列操作系统中可以激活运行：

- Windows 2000、Windows Server 2000
- Windows XP、Windows Server 2003
- Windows Vista
- Windows 7、Windows Server 2008

当它发现自己运行在非 Windows NT 系列操作系统中，会即刻退出。

被攻击的软件系统包括：

- SIMATIC WinCC 7.0
- SIMATIC WinCC 6.2

但不排除其他版本的 WinCC 被攻击的可能。

2.2 本地行为

样本被激活后，典型的运行流程如图 1 所示。

样本首先判断当前操作系统类型，如果是 Windows 9X/ME，就直接退出。

接下来加载一个 DLL 模块，后续要执行的代码大部分都在其中。为了躲避反病毒软件的监视和查杀，样本并不将 DLL 模块释放为磁盘文件，而是直接拷贝到内存中，然后模拟正常的 DLL 加载过程。

具体而言，样本先申请一块内存空间，然后 Hook ntdll.dll 导出的 6 个系统函数：

- ZwMapViewOfSection
- ZwCreateSection
- ZwOpenFile
- ZwClose
- ZwQueryAttributesFile
- ZwQuerySection

为此，样本先修改自身进程内存映像中 ntdll.dll 模块 PE 头的保护属性，然后将偏移 0x40 字节处的一段数据改写为跳转代码表，用以实现对上述函数的 hook。

进而，样本就可以使用修改过的 ZwCreateSection 在内存空间中创建一个新的 PE 节，并将要加载的 DLL 模块拷贝到内存中，最后使用 LoadLibraryW 来获取模块句柄。

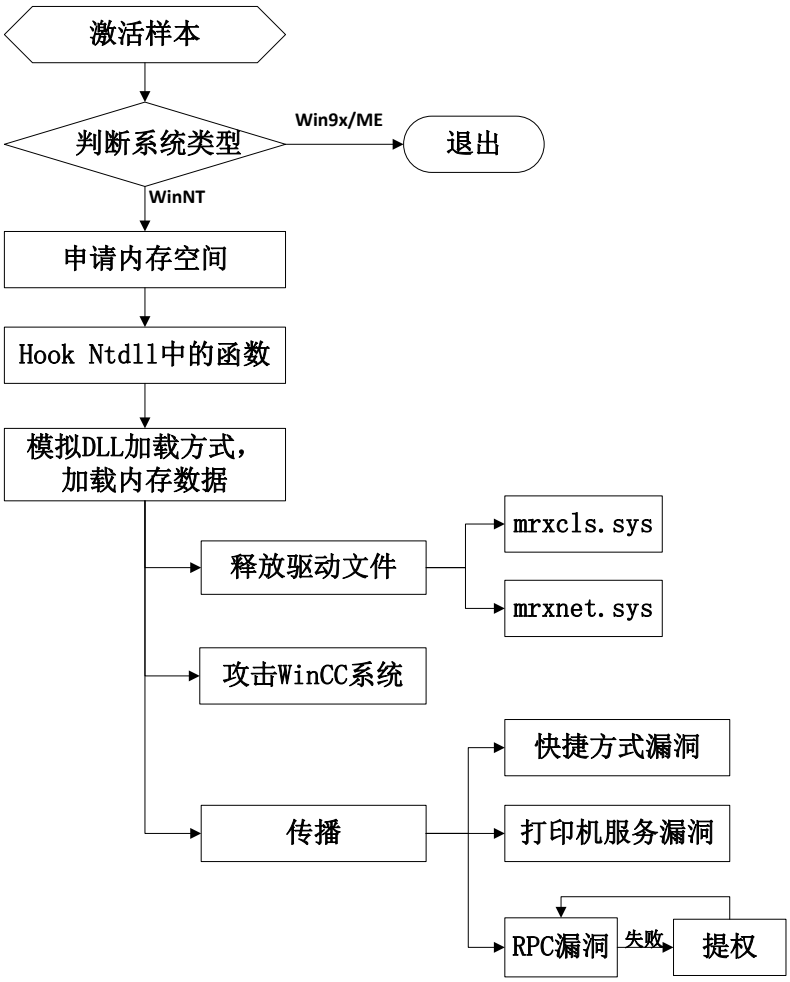


图 1　样本的典型运行流程

此后，样本跳转到被加载的 DLL 中执行，衍生下列文件：

- %System32%\drivers\mrxcls.sys
- %System32%\drivers\mrxnet.sys
- %Windir%\inf\oem7A.PNF
- %Windir%\inf\mdmeric3.PNF
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\oem6C.PNF

其中有两个驱动程序 mrxcls.sys 和 mrxnet.sys，分别被注册成名为 MRXCLS 和 MRXNET 的系统服务，实现开机自启动。这两个驱动程序都使用了 Rootkit 技术，并使用了数字签名。

mrxcls.sys 负责查找主机中安装的 WinCC 系统，并进行攻击。具体地说，它监控系统进程的镜像加载操作，将存储在%Windir%\inf\oem7A.PNF 中的一个模块注入到 services.exe、S7tgtopx.exe、CCProjectMgr.exe 三个进程中，后两者是 WinCC 系统运行时的进程。

mrxnet.sys 通过修改一些内核调用来隐藏被拷贝到 U 盘的 lnk 文件和 DLL 文件（图 2）。

```
loc_11703:                              ; CODE XREF: sub_11688+6A↑j
cmp     esi, 4
jle     short loc_1171D
push    4
lea     eax, [ebx+esi*2-8]
push    eax
mov     eax, offset a_lnk       ; ".LNK"
call    sub_114DA
test    al, al
jnz     short loc_1172F
```

图 2　驱动程序隐藏某些 lnk 文件

2.3　传播方式

Stuxnet 蠕虫的攻击目标是 SIMATIC WinCC 软件。后者主要用于工业控制系统的数据采集与监控，一般部署在专用的内部局域网中，并与外部互联网实行物理上的隔离。为了实现攻击，Stuxnet 蠕虫采取多种手段进行渗透和传播，如图 3 所示。

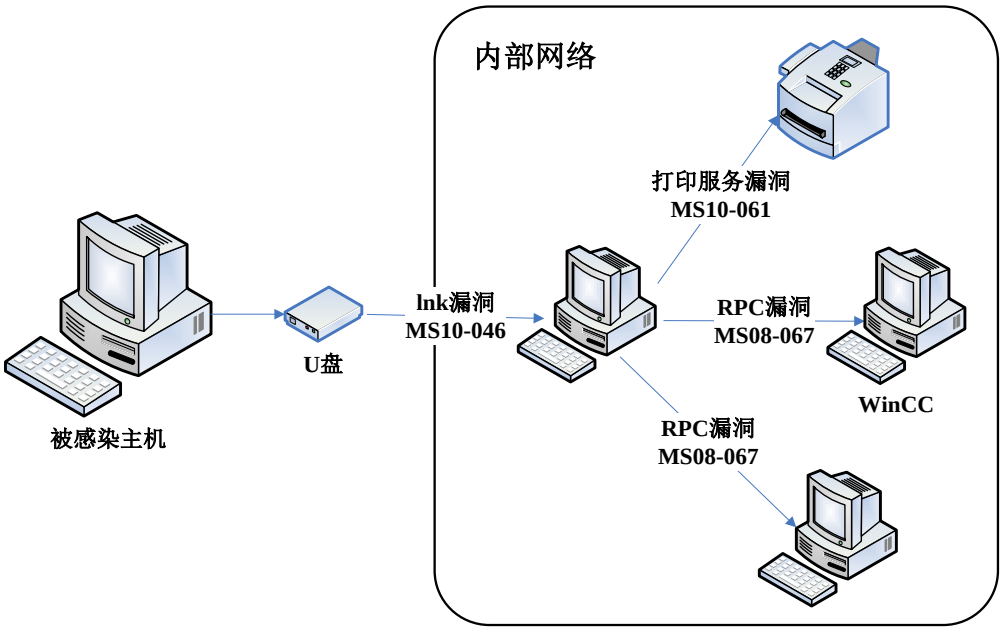


图 3　样本的多种传播方式

整体的传播思路是：首先感染外部主机；然后感染 U 盘，利用快捷方式文件解析漏洞，传播到内部网络；在内网中，通过快捷方式解析漏洞、RPC 远程执行漏洞、打印机后台程序服务漏洞，实现联网主机之间的传播；最后抵达安装了 WinCC 软件的主机，展开攻击。

1.　快捷方式文件解析漏洞（MS10-046）

这个漏洞利用 Windows 在解析快捷方式文件（例如.lnk 文件）时的系统机制缺陷，使系统加载攻击者指定的 DLL 文件，从而触发攻击行为。具体而言，Windows 在显示快捷方式文件时，会根据文件中的结构信息寻找它所需的图标资源，并将其作为文件的图标展现给用户。如果图标资源在一个 DLL 文件中，系统就会加载这个 DLL 文件。攻击者可以构造一个这样快捷方式文件，使系统加载他指定的恶意 DLL 文件，从而触发后者中的恶意代码。快捷方式文件的显示是系统自动执行，无需用户交互，因此漏洞的利用效果很好。

Stuxnet 蠕虫搜索计算机中的可移动存储设备（图 4）。一旦发现，就将快捷方式文件和 DLL 文件拷贝到其中（图 5）。如果用户将这个设备再插入到内部网络中的计算机上使用，就会触发漏洞，从而实现所谓的“摆渡”攻击，即利用移动存储设备对物理隔离网络的渗入。

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&

图 4　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

图 5　拷贝文件到 U 盘

拷贝到 U 盘的 DLL 文件有两个：~wtr4132.tmp 和~wtr4141.tmp。后者 Hook 了 kernel32.dll 和 ntdll.dll 中的下列导出函数：

- FindFirstFileW
- FindNextFileW
- FindFirstFileExW
- NtQueryDirectoryFile
- ZwQueryDirectoryFile

实现对 U 盘中 lnk 文件和 DLL 文件的隐藏。因此，Stuxnet 一共使用了两种措施（内核态驱动程序、用户态 Hook API）来实现对 U 盘文件的隐藏，使攻击过程很难被用户发觉，也能一定程度上躲避杀毒软件的扫描。

2. RPC 远程执行漏洞（MS08-067）与提升权限漏洞

这是 2008 年爆发的最严重的一个微软操作系统漏洞，具有利用简单、波及范围广、危害程度高等特点。

反汇编	文本字串
PUSH Region00.10061C74	ncalrpc:[%s]
PUSH Region00.10061CE0	ncacn_ip_tcp:%s[%u]
PUSH Region00.10061C10	ntsvcs
MOV EBX,Region00.10061C00	browser
PUSH Region00.10061D30	ncacn_ip_tcp
PUSH Region00.10061D08	ncacn_ip_tcp:%s[%s]
PUSH Region00.1005C3FA	h
PUSH Region00.1005C422	h
PUSH Region00.1005C462	h
PUSH Region00.1005C490	h
PUSH Region00.1005C4BE	h
PUSH Region00.1005C5B0	h
PUSH Region00.10061C90	ncacn_np:%s[\\pipe\\%s]
PUSH Region00.10061CC0	ncacn_ip_tcp:%s

图 6　发动 RPC 攻击

具体而言，存在此漏洞的系统收到精心构造的 RPC 请求时，可能允许远程执行代码。在 Windows 2000、Windows XP 和 Windows Server 2003 系统中，利用这一漏洞，攻击者可以通过发送恶意构造的网络包直接发起攻击，无需通过认证地运行任意代码，并且获取完整的权限。因此该漏洞常被蠕虫用于大规模的传播和攻击。

Stuxnet 蠕虫利用这个漏洞实现在内部局域网中的传播（图 6）。利用这一漏洞时，如果权限不够导致失败，还会使用一个尚未公开的漏洞来提升自身权限（图 1），然后再次尝试攻击。截止本报告发布，微软尚未给出该提权漏洞的解决方案。

3. 打印机后台程序服务漏洞（MS10-061）

这是一个零日漏洞，首先发现于 Stuxnet 蠕虫中。

Windows 打印后台程序没有合理地设置用户权限。攻击者可以通过提交精心构造的打印请求，将文件发送到暴露了打印后台程序接口的主机的%System32%目录中。成功利用这个漏洞可以以系统权限执行任意代码，从而实现传播和攻击。

反汇编	注释
MOV EAX,DWORD PTR SS:[EBP+C]	
MOV ECX,DWORD PTR SS:[EBP+10]	
MOV DWORD PTR DS:[EBX+4],EAX	
MOV DWORD PTR DS:[EBX+8],222———?1001681C	winsta.exe
MOV DWORD PTR DS:[EBX+C],ECX	
MOV DWORD PTR DS:[EBX+14],222———?100177A8	
MOV DWORD PTR DS:[EBX+18],222———?10016834	wbem\mof\sysnullevnt.mof
MOV DWORD PTR DS:[EBX+1C],63A	
CALL 222———?10006070	

图 7　利用打印服务漏洞

Stuxnet 蠕虫利用这个漏洞实现在内部局域网中的传播。如图 7 所示，它向目标主机发送两个文件：winsta.exe、sysnullevnt.mof。后者是微软的一种托管对象格式（MOF）文件，在一些特定事件驱动下，它将执行 winsta.exe，也就是蠕虫自身。

2.4　攻击行为

Stuxnet 蠕虫查询两个注册表键来判断主机中是否安装 WinCC 系统（图 8）：

- HKLM\SOFTWARE\SIEMENS\WinCC\Setup
- HKLM\SOFTWARE\SIEMENS\STEP7

HEX 数据																ASCII
53	00	4F	00	46	00	54	00	57	00	41	00	52	00	45	00	S.O.F.T.W.A.R.E.
5C	00	53	00	49	00	45	00	4D	00	45	00	4E	00	53	00	\.S.I.E.M.E.N.S.
5C	00	57	00	69	00	6E	00	43	00	43	00	5C	00	53	00	\.W.i.n.C.C.\.S.
65	00	74	00	75	00	70	00	00	00	00	00	53	00	54	00	e.t.u.p.....S.T.
45	00	50	00	37	00	5F	00	56	00	65	00	72	00	73	00	E.P.7._.V.e.r.s.
69	00	6F	00	6E	00	00	00	53	00	4F	00	46	00	54	00	i.o.n...S.O.F.T.
57	00	41	00	52	00	45	00	5C	00	53	00	49	00	45	00	W.A.R.E.\.S.I.E.
4D	00	45	00	4E	00	53	00	5C	00	53	00	54	00	45	00	M.E.N.S.\.S.T.E.
50	00	37	00	00	00	00	00	00	00	00	00	53	00	4F	00	P.7.........S.O.

图 8　查询注册表，判断是否安装 WinCC

一旦发现 WinCC 系统，就利用其中的两个漏洞展开攻击：

一是 WinCC 系统中存在一个硬编码漏洞，保存了访问数据库的默认账户名和密码，Stuxnet 利用这一漏洞尝试访问该系统的 SQL 数据库（图 9）。

二是在 WinCC 需要使用的 Step7 工程中，在打开工程文件时，存在 DLL 加载策略上的缺陷，从而导致一种类似于“DLL 预加载攻击”的利用方式。最终，Stuxnet 通过替换 Step7 软件中的 s7otbxdx.dll，而将原来的同名文件修改为 s7otbxsx.dll，并对这个文件的导出函数进行一次封装，从而实现对一些查询、读取函数的 Hook。

文本字串

```
declare @t varchar(4000), @e int, @f int if exists (select text from dbo
declare @t varchar(4000), @e int, @f int if exists (select * from dbo.sy
use master
.mdf
select name from master..sysdatabases where filename like n'%s'
.mdf
.ldf
exec master..sp_attach_db 'wincc_svr',n'%s',n'%s'
exec master..sp_detach_db 'wincc_svr'
use wincc_svr
exec master..sp_detach_db 'wincc_svr'
.mdf
.ldf
 ((select top 1 1 from mcpvreadvarpercon)='1') --cc-sp
x
0
.mdf
.mdf
vector<t> too long
2wsxcder
winccconnect
master
.\wincc
sqloledb
provider='%s';data source=%s;initial catalog='%s';user id='%s';password=
```

图 9　查询 WinCC 的数据库

2.5　样本文件的衍生关系

本节综合介绍样本在上述复制、传播、攻击过程中，各文件的衍生关系。

如图 10 所示。样本的来源有多种可能。

对原始样本、通过 RPC 漏洞或打印服务漏洞传播的样本，都是 exe 文件，它在自己的.stud 节中隐形加载模块，名为“kernel32.dll.aslr.<随机数字>.dll”。

对 U 盘传播的样本，当系统显示快捷方式文件时触发漏洞，加载~wtr4141.tmp 文件，后者加载一个名为“shell32.dll.aslr.<随机数字>.dll”的模块，这个模块将另一个文件~wtr4132.tmp 加载为“kernel32.dll.aslr.<随机数字>.dll”。

模块“kernel32.dll.aslr.<随机数字>.dll”负责实现后续的大部分攻击行为，它导出了 22 个函数来完成恶意代码的主要功能；在其资源节中，包含了一些衍生文件，它们以加密的形式被保存。

其中，第 16 号导出函数用于衍生一些本地文件，包括资源编号 201 的 mrxcls.sys 和编号 242 的 mrxnet.sys 两个驱动程序，以及 4 个.pnf 文件。

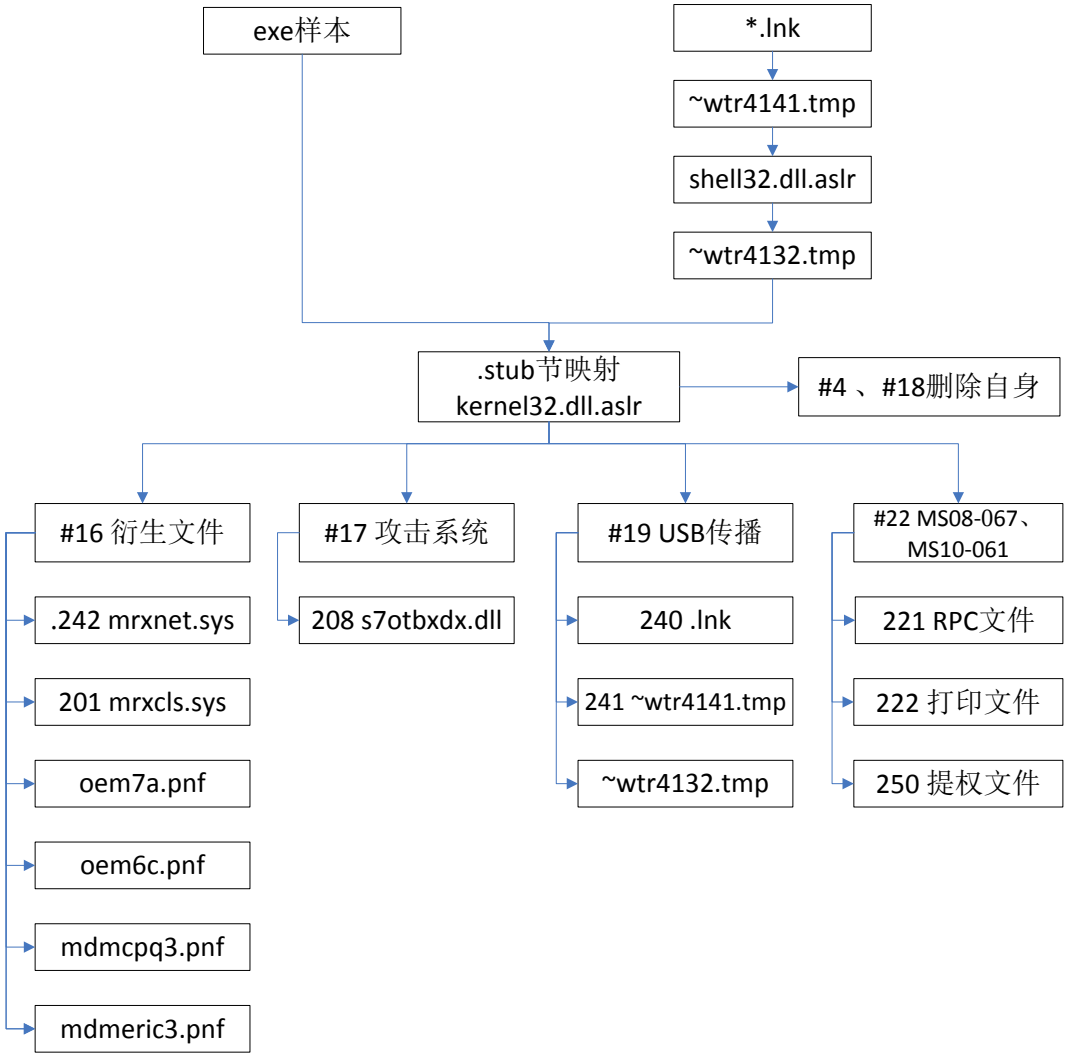


图 10　样本文件衍生的关系

第 17 号导出函数用于攻击 WinCC 系统的第二个漏洞，它释放一个 s7otbxdx.dll。

第 19 号导出函数负责利用快捷方式解析漏洞进行传播。它释放多个 lnk 文件和两个扩展名为 tmp 的 DLL 文件。

第 22 号导出函数负责利用 RPC 漏洞和打印服务漏洞进行传播。它释放的文件中，资源编号 221 的文件用于 RPC 攻击、编号 222 的文件用于打印服务攻击、编号 250 的文件用于提权。

3 解决方案与安全建议

3.1 抵御本次攻击

西门子公司对此次攻击事件给出了解决方案，链接地址见附录。下面根据我们的分析结果，给出更具体的措施。

1. 使用相关专杀工具或手工清除 Stuxnet 蠕虫

手工清除的步骤为：

1) 使用安天 Atool 工具，结束系统中的父进程不是 winlogon.exe 的所有 lsass.exe 进程；

2) 强行删除下列衍生文件：

- %System32%\drivers\mrxcls.sys
- %System32%\drivers\mrxnet.sys
- %Windir%\inf\oem7A.PNF
- %Windir%\inf\mdmeric3.PNF
- %Windir%\inf\mdmcpq3.PNF
- %Windir%\inf\oem6C.PNF

3) 删除下列注册表项：

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNET

2. 安装被利用漏洞的系统补丁

安装微软提供的下列补丁文件：

- RPC 远程执行漏洞（MS08-067）
- 快捷方式文件解析漏洞（MS10-046）
- 打印机后台程序服务漏洞（MS10-061）

此外，需要注意还有一个尚未修补的提升权限（EoP）漏洞，以及微软随后发现的另一个类似漏洞。用户需对这两个漏洞的修补情况保持关注。

3. 安装软件补丁

安装西门子发布的 WinCC 系统安全更新补丁，下载地址见附录。

3.2 安全建议

此次攻击事件凸显了两个问题：

1. 即便是物理隔离的专用局域网，也并非牢不可破；
2. 专用的软件系统，包括工业控制系统，也有可能被攻击。

因此，我们对有关部门和企业提出下列安全建议：

- 加强主机（尤其是内网主机）的安全防范，即便是物理隔离的计算机也要及时更新操作系统补丁，建立完善的安全策略；
- 安装安全防护软件，包括反病毒软件和防火墙，并及时更新病毒数据库；
- 建立软件安全意识，对企业中的核心计算机，随时跟踪所用软件的安全问题，及时更新存在漏洞的软件；
- 进一步加强企业内网安全建设，尤其重视网络服务的安全性，关闭主机中不必要的网络服务端口；
- 所有软件和网络服务均不启用弱口令和默认口令；
- 加强对可移动存储设备的安全管理，关闭计算机的自动播放功能，使用可移动设备前先进行病毒扫描，为移动设备建立病毒免疫，使用硬件式 U 盘病毒查杀工具。

4 攻击事件的特点

相比以往的安全事件，此次攻击呈现出许多新的手段和特点，值得特别关注。

4.1 专门攻击工业系统

Stuxnet 蠕虫的攻击目标直指西门子公司的 SIMATIC WinCC 系统。这是一款数据采集与监视控制（SCADA）系统，被广泛用于钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域，特别是国家基础设施工程；它运行于 Windows 平台，常被部署在与外界隔离的专用局域网中。

一般情况下，蠕虫的攻击价值在于其传播范围的广阔性、攻击目标的普遍性。此次攻击与此截然不同，最终目标既不在开放主机之上，也不是通用软件。无论是要渗透到内部网络，还是挖掘大型专用软件的漏洞，都非寻常攻击所能做到。这也表明攻击的意图十分明确，是一次精心谋划的攻击。

4.2 利用多个零日漏洞

Stuxnet 蠕虫利用了微软操作系统的下列漏洞：

1. RPC 远程执行漏洞（MS08-067）

2. 快捷方式文件解析漏洞（MS10-046）
3. 打印机后台程序服务漏洞（MS10-061）
4. 尚未公开的一个提升权限漏洞

后三个漏洞都是在 Stuxnet 中首次被使用，是真正的零日漏洞。如此大规模的使用多种零日漏洞，并不多见。

这些漏洞并非随意挑选。从蠕虫的传播方式来看，每一种漏洞都发挥了独特的作用。比如基于自动播放功的 U 盘病毒被绝大部分杀毒软件防御的现状下，就使用快捷方式漏洞实现 U 盘传播。

另一方面，在安天捕获的样本中，有一部分实体的时间戳是今年 3 月。这意味着至少在 3 月份，上述零日漏洞就已经被攻击者掌握。但直到 7 月份大规模爆发，漏洞才首次披露出来。这期间要控制漏洞不泄露，有一定难度。

4.3 使用有效的数字签名

Stuxnet 在运行后，释放两个驱动文件：

- %System32%\drivers\mrxcls.sys
- %System32%\drivers\mrxnet.sys

这两个驱动文件使用了 RealTek 的数字签名（图 11）以躲避杀毒软件的查杀。目前，这一签名已经被颁发机构吊销，无法再通过在线验证，但目前反病毒产品大多使用静态方法判定可执行文件是否带有数字签名，因此有可能被欺骗。

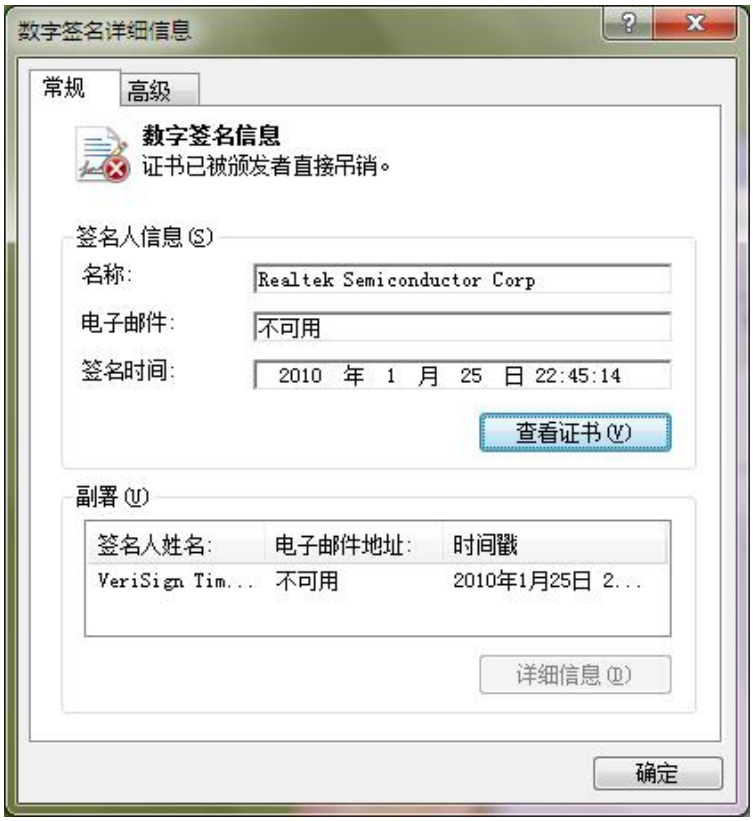


图 11 Stuxnet 使用的数字签名

4.4 明确的攻击目标

根据赛门铁克公司的统计，7 月份，伊朗感染 Stuxnet 蠕虫的主机只占 25%，到 9 月下旬，这一比例达到 60%。

WinCC 被伊朗广泛使用于基础国防设施中。9 月 27 日，伊朗国家通讯社向外界证实该国的第一座核电站“布什尔核电站”已经遭到攻击。据了解，该核电站原计划于今年 8 月开始正式运行。而 Stuxnet 编写于 3 月，直到 7 月才大规模爆发，与这一计划不谋而合。因此，有充分的理由相信此次攻击具有明确的地域性和目的性。

5 综合评价

5.1 工业系统安全将面临严峻挑战

在我国，WinCC 系统已经广泛应用于很多重要行业，一旦受到攻击，可能造成相关企业和工程项目的基础设施运转出现异常，甚至发生机密失窃、停工停产等严重事故。

对 Stuxnet 蠕虫的出现，我们并未感到十分意外。早在一年多以前，安天就接受用户委托，对化工行业仪表的安全性展开过类似的分析研究，结论不容乐观。

工业控制网络，包括工业以太网、现场总线控制系统，在工业企业中早已应用多年。目前在电力、钢铁、化工等大型重化工业企业中，工业以太网、DCS（集散控制系统）、现场总线等技术早已渗透到控制系统的方方面面。工业控制网络的核心现在都是工控 PC，大多数同样基于 Windows-Intel 平台；工业以太网与民用以太网在技术上并无本质差异；现场总线技术更是将单片机与嵌入式系统应用到了每一个控制仪表上。工业控制网络除了可能遭到与攻击民用或商用网络手段相同的攻击，例如通过局域网传播的恶意代码之外，还可能遭到针对现场总线的专门攻击。

针对民用或商用计算机和网络的攻击，目前多以获取经济利益为主要目标；但针对工业控制网络和现场总线的攻击，则可能破坏企业重要装置和设备的正常测控，由此引起的后果将是灾难性的。以化工行业为例，针对工业控制网络的攻击可能破坏反应器的正常温度与压力测控，导致反应器超温或超压，最终就会导致冲料、起火甚至爆炸等灾难性事故，还可能造成次生灾害和人道主义灾难。因此，这种袭击工业网络的恶意代码一般带有信息武器的性质，目标是对重要工业企业的正常生产进行干扰甚至严重破坏，其发起者一般不是个人或者普通地下黑客组织。

目前，工业以太网和现场总线标准均为公开标准，熟悉工控系统的程序员开发针对性的恶意攻击代码并不存在很高的技术门槛。因此，对下列可能的工业网络安全薄弱点进行增强和防护是十分必要的：

基于 Windows-Intel 平台的工控 PC 和工业以太网。可能遭到与攻击民用或商用 PC 和网络手段相同的攻击，例如通过 U 盘传播恶意代码和网络蠕虫。

DCS 和现场总线控制系统中的组态软件（测控软件的核心）。针对组态软件的攻击会从根本上破坏测控体系。目前，这类产品，特别是行业产品，被少数公司所垄断，例如电力行业常用的西门子 SIMATIC WinCC、石化行业常用的浙大中控等。

随着现场总线的进一步广泛应用，基于数字通信的现场总线将成为新的攻击目标，攻击现场总线的危害性不次于攻击工业以太网。基于 RS-485 总线以及光纤物理层的现场总线，例如 PROFIBUS 和 MODBUS（串行链路协议），其安全性相对较好；但短程无线网络，尤其是不使用 Zigbee 等通用短程无线协议（有一定的安全性），而使用自定义专用协议的短程无线通信测控仪表，安全性较差。特别是国内一些小企业生产的“无线传感器”等测控仪表，其无线通信部分采用通用 2.4GHz 短程无线通信芯片，连基本的加密通信都没有使用，可以说毫无安全性可言，极易遭到窃听和攻击，如果使用，将成为现场总线中最容易被攻击的薄弱点。

相对信息网络而言，传统工业网络的安全一直是凭借内网隔离，而疏于防范。因此，针对工业系统的安全检查和安全加固迫在眉睫。

5.2 展望和思考

在传统工业与信息技术的融合不断加深、传统工业体系的安全核心从物理安全向信息安全转移的趋势和背景下，此次 Stuxnet 蠕虫攻击事件尤为值得我们深入思考。

这是一次极为不同寻常的攻击，其具体体现是：

- 传统的恶意攻击追求影响范围的广泛性，而这次攻击极富目的性；
- 传统的攻击大都利用通用软件的漏洞，而这次攻击则完全针对行业专用软件；
- 这次攻击使用了多个全新的零日漏洞进行全方位攻击，这是传统攻击难以企及的；
- 这次攻击通过恰当的漏洞顺利渗透到内部专用网络中，这也正是传统攻击的弱项；
- 从时间、技术、手段、目的、攻击行为等多方面来看，完全可以认为发起此次攻击的不是个人或者普通地下黑客组织。

因此，这次攻击中所采用的多个新漏洞和传播手段，将在接下来很长一段时间内给新的攻击提供最直接的动力。至少有两种新的攻击趋势值得注意：

1. 针对行业专用软件的漏洞挖掘和攻击，特别是对上升到国家战略层面的关键行业和敏感行业的专用软件的攻击。安天实验室在今年年初发布的《多家企业网络入侵事件传言的同源木马样本分析报告》中就明确指出：“目前的漏洞分析挖掘的注意点已经不集中于主流厂商，而开始普遍扩散”。另一方面，这些攻击虽然针对软件，但并不一定就是利用软件本身的缺陷，安全是全方位的问题，攻击可能来自于任何一个角度。
2. 针对企业内部网络，特别是物理隔离的内部专用网络的攻击。这类网络具有较高的安全要求，也更具攻击价值。通过 U 盘等可移动存储设备渗入这类网络的常用方法和技术包括感染、欺骗、自动播放等。本次出现的快捷方式文件解析漏洞，为此类攻击提供了一种更有效的方法。此外，这种内部网络也将因为本次事件而被攻击者关注和研究，不能排除出现新的攻击方式的可能。

在对病毒未来发展的种种预言中，最令人恐惧的还不是它对计算机节点自身数据的影响，而在于它对相关环节可能产生的关联影响，比如对武器系统的非法控制等等。不幸的是，此次 Stuxnet 蠕虫攻击事件就证明：如果没有有效的防范，上述预言就一定会变成事实。

工业电子化体系的第一次进步是模拟电子技术与机械制造技术的结合。此后，随着数字化技术的不断引入，依托单片机、嵌入式程序及早期数字化工业控制协议，它完成了第二次跳跃。此时的工业控制系统与办公信息网络异构并且分离，其安全考虑以物理安全为主。

随着 PC 环境、互联网络的成本逐渐降低，越来越多的工业系统和其它信息系统开始走向标准的 x86 环境，越来越多的控制信号和采集传输开始采用 TCP/IP 协议标准甚至使用公网传输，这就让庞大的 x86 病毒

种群找到了可能带来更致命威胁的新目标。因此，即便采用基于传统物理隔离的数据交换也不能绝对保证安全，本次事件中，U 盘这种非实时传播途径带来的威胁就再次凸显。另一方面，出于内网隔离和稳定性考虑，工业系统常使用版本较老的操作系统，且没有有效的补丁条件，这更加剧了安全隐患。

传统工业系统的设计者和使用者，在物理安全方面已经作出了很多考量，通过足够多的传感器、大量的流程、文献、以及人的积极努力来保证工业系统的正常运行。而本次事件中，系统开发人员把连接数据库的用户名和口令做成硬编码，而不是与程序独立的可配置内容，这是软件开发中的一种低级失误，却可能普遍存在于目前的专用软件系统中。我们可以看到，在安全方面，传统 PC 开发走过的每一条弯路，在工业控制系统基本都会重演。也可以判定，在未来的 20 年内，工业系统的安全问题核心已不再是孤立的物理和实体安全问题，而是作为其运转灵魂的信息系统的安全问题。而这个问题更大地存在于人类视为未来发展和前进方向的物联网之上。

安全厂商并没有被视为传统工业安全体系中的一员。因此，本次事件的初期，安全厂商与攻击者处在信息不对称的位置。攻击者针对目标工业系统进行了长期的分析和准备，然后发动攻击；而当安全厂商面对突发事件，却并不能像常用操作系统或互联网软件出现漏洞时一样，在第一时间重现问题并跟进分析，而必须得到有关软件开发商的配合。从这个角度来看，利用 PC 环境的通用性传播，然后对相对封闭的工业系统或者其他专用系统展开攻击，利用制造厂商与安全厂商之间的信息不对称来获得有效攻击时间，这将成为一种新的、具有极大挑战和讽刺意味的攻击方法。因此，认为专有体系独立于安全威胁之外的错误观念，导致对安全厂商的拒之门外的行为，实际上反而是对攻击者的开门揖盗。

作为职业的安全工程师，我们将积极主动地承担更大的责任。未来将证明，我们的工作不仅是在保护一个虚拟的世界，也在保护着我们赖以生存的真实世界。

附录一：参考资料

[1] 西门子公司就此次攻击给出的解决方案：
http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objid=43876783

[2] 微软提供的补丁文件下载地址如下：

- RPC 远程执行漏洞（MS08-067）
  http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx
- 快捷方式文件解析漏洞（MS10-046）
  http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx
- 打印机后台程序服务漏洞（MS10-061）
  http://www.microsoft.com/technet/security/bulletin/MS10-061.mspx

[3] 西门子公司给出的 WinCC 系统安全更新补丁的下载地址：
http://support.automation.siemens.com/WW/llisapi.dll/csfetch/43876783/SIMATIC_Security_Update_V1_0_0_11.exe?func=cslib.csFetch&nodeid=44473682

[4] 安天 ATool 工具下载地址：
http://www.antiyfx.com/download/atool.zip

[5] 安天实验室发布的《多家企业网络入侵事件传言的同源木马样本分析报告》：
http://www.antiy.com/cn/security/2010/s100128_002.htm

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）
http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访 http://www.antiy.cn

问：

附录三：安天应急响应时间表

时间	工作内容
2010.07.15	安天捕获到 Stuxnet 的第一个变种，随即更新安天防线病毒库，实现查杀
2010.07.20	对 Stuxnet 样本和快捷方式漏洞展开分析
2010.07.23	形成初步分析报告
2010.08.18	正式发布分析报告与防范措施
2010.07.15-2010.09.28	持续捕获样本，跟踪事件变化
2010.09.27	发布本报告第一版
2010.09.28	发布本报告第二版、第三版
2010.09.29	修订本报告第三版，发布本报告英文版
2010.09.30	再次修订本报告第三版