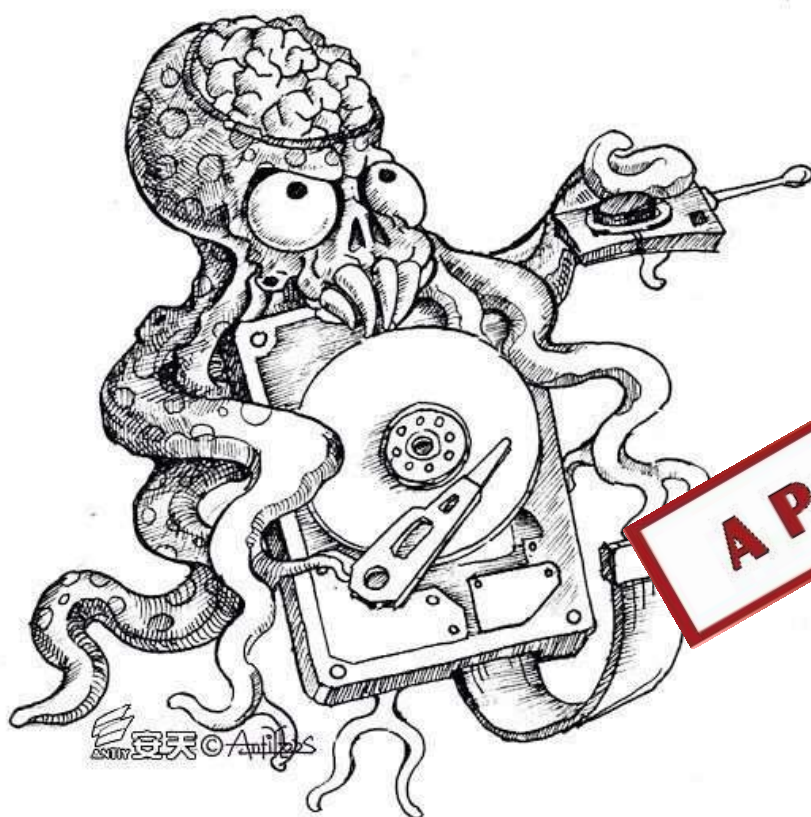


方程式组织 EQUATION DRUG 平台解析

——方程式组织系列分析报告之四

安天安全研究与应急处理中心 (Antiy CERT)



报告初稿完成时间：2017 年 1 月 13 日 16 时 00 分

首次发布时间：2017 年 1 月 16 日 10 时 00 分

本版本更新时间：2017 年 1 月 25 日 14 时 30 分

目 录

1	本版本更新小语.....	1
2	背景.....	1
3	方程式线索曝光和分析成果时间链梳理.....	2
4	DANDERSPRITZ 攻击平台	4
5	部分组件与插件分析（继续完善中）	11
5.1	PROCESSINFO 插件遍历进程模块	13
5.2	KILL_IMPLANT 插件杀进程模块	16
5.3	GROK 键盘与剪贴版记录器驱动	16
6	小结.....	20
	附录一：参考资料.....	22
	附录二：关于安天.....	24

1 本版本更新小语

安天在此前发布的报告版本的基础上，增加了一个方程式组织主机作业模块的积木图。这个积木图初步展示了一个将主机情报作业按照“原子化”拆分的模块组合的拼装，在本版本中安天 CERT 也细化了对部分模块的分析，尽管目前的分析只覆盖这些模块的一少部分。

在数天前，安天 CERT 把这份暂时称为“提纲”的未完成分析结果发布出来，这并非因为我们期望“速战速决”，而草率地发布一点粗浅的进展，而是我们需要获得更多的建议和批判。所幸的是，在上一版本发布后，获得了业内专家中肯而尖锐的批评，让安天认识到，在面对这组 2007~2008 年的攻击模块集合时，分析小组再次出现了和当年分析“火焰”时一样的迷茫（尽管安天曾经一度以为自己比那时更清晰）。这些庞杂的模块展开了一组拼图碎片，每一张图上都是有意义的图案，但如果逐一跟进进去，这些图案就会组成一个巨大的迷宫。迷宫之所以让人迷惑，不在于其处处是死路，而在于其看起来处处有出口，但所有的砖块都不能给进入者以足够的提示。此时，最大的期待，不只是有一只笔，可以在走过的地方做出标记，而是插上双翼凌空飞起，俯瞰迷宫的全貌。当然这是一种提升分析方法论的自我期待，我辈当下虽身无双翼，但或可练就一点灵犀。

目前安天的积木还原工作还刚刚起步，对于能够在中国的传统节日春节前，发布出分析报告的新版本，安天还是有些许欣慰的。网络安全注定是一个需要永远保持警惕和勤奋的行业，我们的分析工作会持续进行下去，即使是在焰火升腾，鞭炮响起的时刻，依然需要有紧盯反汇编代码和威胁态势的眼睛。

感谢业内专家同仁对安天的关注和支持，感谢安天客户对安天产品与服务的信任，祝大家新春快乐！

2 背景

对于方程式组织，在过去的两年中，安天已经连续发布了三篇分析报告：在《修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件》^[1]中，安天对多个模块进行了分析，并对其写入硬盘固件的机理进行了分析验证；在《方程式（EQUATION）部分组件中的加密技巧分析》^[2]报告中，对攻击组件中使用的加密方式实现了破解；在《从“方程式”到“方程组”——EQUATION 攻击组织高级恶意代码的全平台能力解析》^[3]报告中，安天独家提供了方程式在 Linux 和 Solaris 系统的样本分析，这也是业内首次正式证实这些“恶灵”真实存在的公开分析。

APT 的分析成果，与研发反 APT 产品一样，都要基于充分的基础积累，而不可能“一夜之间建成罗马”。对于方程式这样大至无形的超级攻击组织来说，安天过去所做的具体的分析工作都是盲人摸象的过程，一旦飘忽的线索落入安天已经摸索过的范围之内，就可以迅速发布储备成果，而如果面对的是一个未曾充分

探查的区域，则需要更长的时间展开分析工作，因此与安天此前已经发布的三篇方程式的长篇报告相比，本篇报告目前的版本依然是比较仓促的，因此安天会坚持称之为“提纲”，旨在能抛砖引玉，邀请更多兄弟团队共同加入分析工作，以便进一步呈现出其全貌。

本篇展现的分析工作是围绕 2017 年 1 月 12 日“影子经纪人”放出 Equation Group 组件中的 61 个文件^[4]而展开的。经分析，在本次放出的 61 个文件中，其中含有 Equation Group 组件和 DanderSpritz (RAT) 工具中的一些插件。DanderSpritz 是 NSA (National Security Agency) 的间谍工具之一，在 1 月 7 号“影子经纪人”放出的 Windows 攻击工具^[5]中也包含了大量 DanderSpritz 的插件名称。

组件 EquationDrug 是一个很复杂的模块，其存活时间有近 10 年，后来被 GrayFish 升级替代。从 EquationDrug 到 GrayFish 是攻击平台级别的恶意代码体系，具有安装与卸载插件功能。在本次“影子经纪人”放出的文件中，安天 CERT 看到了更多的 EquationDrug 组件中的插件。通过分析比对发现，这些插件比之前安天分析过的插件版本低，但其中包含了一些此前未曾被业内捕获到的模块。

3 方程式线索曝光和分析成果时间链梳理

从 2013 年起，安天从样本分析中，逐步发现存在一个拥有全平台载荷攻击能力的攻击组织，并逐步关联分析了其多个平台的样本。在这个过程中，安天感到一个大至无形的超级攻击组织的存在，但并未找到其攻击背景。

2015 年 2 月，卡巴斯基实验室曝光了一个名为方程式 (Equation Group)^[6]的攻击组织，引发了全球关注，卡巴斯基认为该组织已活跃近 20 年，可能是目前世界上存在的最复杂的 APT 攻击组织之一，并认为该组织是震网 (Stuxnet) 和火焰 (Flame) 病毒幕后的操纵者。经过线索比对，安天发现这正是此前一直跟踪的超级攻击组织，决定通过报告公开其针对硬盘固件作业的原理^[1]和已破解的其部分加密算法^[2]，形成了安天对于方程式系列分析的前两篇报告。

2015 年 3 月，卡巴斯基实验室发布了基于 Equation Drug 组件或平台的剖析^[7]，Equation Drug 是方程式组织所用的主要间谍组件或平台之一，最早可追溯到 2001 年，并且一直沿用至今。该组件或平台的架构类似于一个具有内核模式和用户模式的微型操作系统，通过自定义接口进行交互。该组件或平台包括驱动程序、平台内核 (协调器) 和若干插件，其中一些插件配备独特的 ID 和版本号，用于定义相关功能等。

2016 年 8 月，一个自称“影子经纪人” (The Shadow Brokers) 的个人 (或组织) 声称入侵了网络间谍组织方程式 (Equation)^[8]，并以 100 万比特币 (当时约价值为 5.6 亿美元) 的价格，公开“拍卖”所掌握的方程式组织的攻击工具，方程式组织被认为与 NSA 存在联系。为证明成功入侵的真实性，“影子经纪人”

于当月 13 日在开源项目托管平台 GitHub 加密发布了这些攻击工具，并有意将其中的少量攻击工具以明文形式发布。

2016 年 8 月，卡巴斯基实验室通过对方程式组织与“影子经纪人”曝光的数据进行对比验证^[9]，确认了曝光的数据与方程式组织有关。2016 年 10 月，“影子经纪人”对攻击工具再度发起拍卖^[10]，并称在 GitHub 发布的方程式攻击工具只占其掌握的 60%。

2016 年 11 月，“影子经纪人”公开了一份遭受入侵的服务器清单^[11]，并称攻击方与 NSA 有关。清单的日期显示，各系统遭受入侵的时间是在 2000 年到 2010 年之间，受控 IP 及域名分布在 49 个国家，主要集中在亚太地区，受影响的国家包括中国、日本、韩国、西班牙、德国、印度等。安天将这些数据导入到安天态势感知和预警平台，形成了下图的可视化展现。

在“影子经纪人”的爆料中，提及的相关服务器可能是 Linux、FreeBSD 和 Solaris。而在 2016 年上半年的两次技术会议中，安天则明确说明，方程式有针对多个系统平台的样本，其中包括 Linux 和 Solaris。安天最终于 2016 年 11 月 5 日公开了方程式组织针对 Linux 和 Solaris 的部分样本载荷的分析报告（安天方程式系列报告之三）^[3]。



图 3-1 安天态势感知与监控预警平台：方程式组织对全球互联网节点的入侵可视化复现

安天分析团队小组对方程式的上述信息进行了梳理，整理出方程式事件曝光和相关分析的时间链。

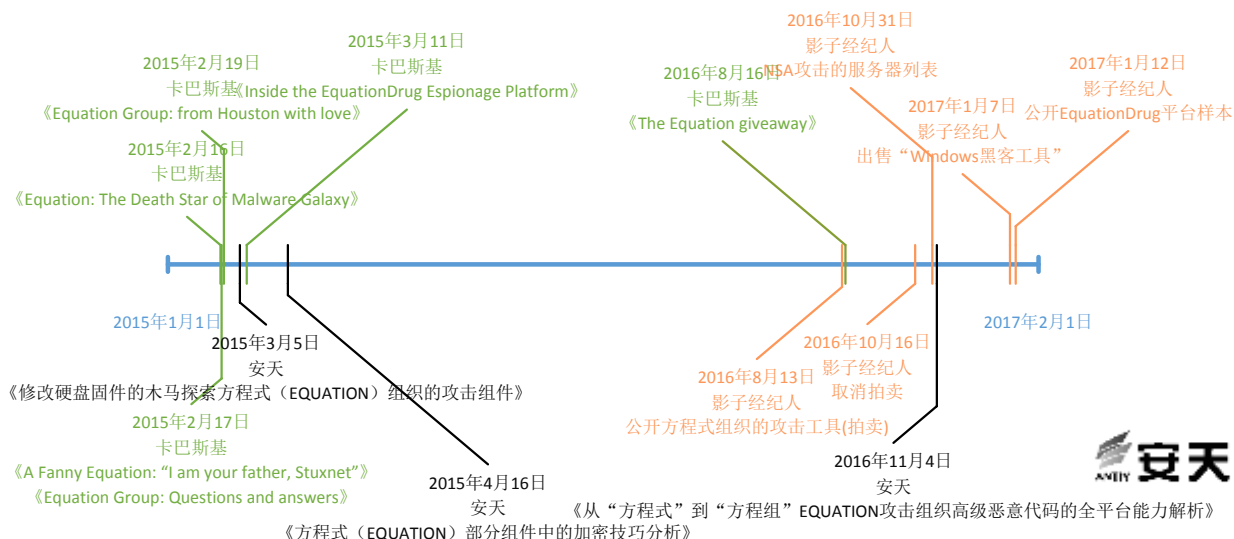


图 3-2 方程式事件相关信息曝光和厂商分析的时间链

4 DanderSpritz 攻击平台

安天通过对本次泄露的文件以及对以往方程式资料的分析发现，方程式组织的“EquationDrug”平台与泄露文件中提到的“DanderSpritz”具有一定内在联系：

1. 本次泄露的 msgkd.ex_、msgki.ex_、msgks.ex_、msgku.ex_ 为 GROK 插件，是“DanderSpritz”的插件或模块，该插件在“EquationDrug”平台中也曾出现，通过分析发现本次泄露的 GROK 为低版本 GROK 插件。
2. 本次曝光的各类 DLL 插件中的一处数据为插件 ID，插件 ID 都是以 0x79 开头，如：0x79A4、0x79D8，同样，“EquationDrug”平台的插件也设有内置 ID，“EquationDrug”平台的插件 ID 为 0x80 开头，且两个平台的插件导出函数参数的数据结构也存在相似之处。

因此，基本可以认为方程式组织使用的“EquationDrug”攻击平台与“DanderSpritz”使用了相同的架构设计，两者可能是不同的版本代号，或至少来自同一开发团队或资源高度共享的团队。

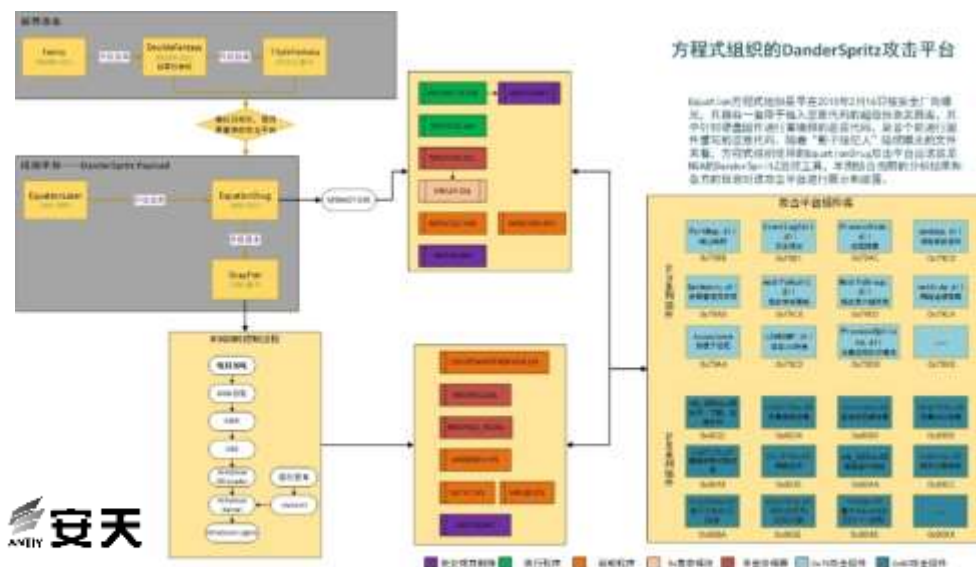


图 4-1 方程式组织的 DanderSpritz 攻击平台

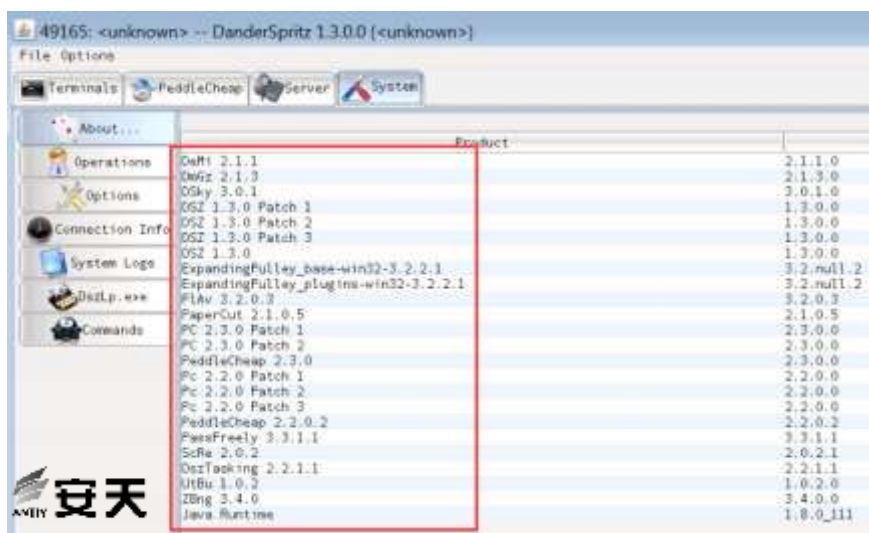


图 4-2 “影子经纪人”泄露的“DanderSpritz”攻击平台截图

本次“影子经纪人”所曝光的文件中多数为“DanderSpritz”平台的攻击插件，一是文件列表，二是 61 个部分插件实体文件。从放出的文件列表 HASH 和截图来看，攻击工具和插件非常丰富且标准化，具体包括远控、漏洞利用、后门、插件等。DanderSpritz_All_Find.txt 文件内容多达 7 千余行，其中插件有数百个之多。对泄露出来的 61 个文件进行分析梳理，根据样本中的一些信息推断，这 61 个样本应该属于两类：测试版本与发布版本。测试版本中含有一些明文信息，并没有进行加密处理，使用了常规的函数调用方式，而在发布版本中这些信息并不存在，函数调用方式也改为动态调用，更加隐蔽。从时间戳上来看，测试版本的生成时间比发布版本要早 5 秒左右。测试版本是不应用于实际攻击中的，从侧面也再次证实了这些文件是被从开发和保管场景窃取出来的，而不是在攻击中捕获到的。

表 4-1 泄露实体文件的部分插件功能列表

测试版本	发布版本	功能
	DoubleFeatureDll.dll.unfinalized	该模块用于创建线程执行函数，地址由调用者传入。同时，内部还有 SHA256、AES、CRC32 等算法。
DuplicateToken_Lp.dll	DuplicateToken_Implant.dll	该模块用于获取 Token，并执行操作。
	DXGHLP16.SYS	该模块用于网络嗅探监测以太网和 VPN 的流量，用于 Windows 9x 系统。
EventLogEdit_Lp.dll	EventLogEdit_Implant.dll	该模块可对事件日志文件进行编辑。
GetAdmin_Lp.dll	GetAdmin_Implant.dll	该模块用于获取管理员权限，并执行操作。
	kill_Implant.dll	该模块功能是结束进程，传入参数中有要结束进程的 ID，该功能的实现使用了常规的系统函数，如：OpenProcess、TerminateProcess。
	kill_Implant9x.dll	该模块功能与 kill_Implant.dll 相同，是针对 64 位系统的版本。
LSADUMP_Lp.dll	LSADUMP_Implant.dll	该模块可用来读取 LSA 凭据，根据传入参数的不同执行不同的操作。
modifyAudit_Lp.dll	modifyAudit_Implant.dll	该模块用于修改审核配置。
modifyAuthentication_Lp.dll	modifyAuthentication_Implant.dll	该模块用于修改权限认证。
ModifyGroup_Lp.dll	ModifyGroup_Implant.dll	该模块用于修改用户组权限。
ModifyPrivilege_Lp.dll	ModifyPrivilege_Implant.dll	该模块用于修改用户权限。
	msgkd.ex_	释放 GROK 键盘/剪贴板记录器驱动。
	msgki.ex_	
	msgks.ex_	
	msgku.ex_	
	mstcp32.sys	该模块用于网络嗅探监测以太网和 VPN 的流量。
nethide_Lp.dll	nethide_Implant.dll	该模块用于隐藏网络连接。
	ntevt.sys	该模块是事件日志相关驱动。
	ntevtx64.sys	该模块功能与 ntevt.sys 相同，是针对 64 位系统的版本。
PortMap_Lp.dll	PortMap_Implant.dll	该模块进行端口映射。
ProcessHide_Lp.dll	ProcessHide_Implant.dll	该模块可以进行隐藏进程，恢复隐藏的进程，根据传入参数的不同执行不同的操作。
	processinfo_Implant.dll	该模块可以用来获取进程信息。
	processinfo_Implant9x.dll	该模块功能与 processinfo_Implant.dll 相同，是针对 64 位系统的版本。
ProcessOptions_Lp.dll	ProcessOptions_Implant.dll	该模块用于设定进程执行属性。
pwdump_Lp.dll	pwdump_Implant.dll	该模块可用来读取系统中密码，根据传入参数的不同执行不同的操作。
RunAsChild_Lp.dll	RunAsChild_Implant.dll	该模块用于创建子进程，并执行操作。
	tdi6.sys	该模块用于网络嗅探监测以太网和 VPN 的流量。
PassFreely_LP.dll	PassFreely_Implant.dll	正在分析中
...		

表 4-2 仅泄露文件名的部分插件功能猜测

测试版本	发布版本	猜测功能
Users_Lp.dll	Users_Implant.dll	查看当前用户列表
GroupUsers_Lp.dll	GroupUsers_Implant.dll	修改指定用户所在组
	nc.exe	nc 网络工具
ProcessCheck_Lp.dll	ProcessCheck_Implant.dll	检测指定进程
machineinfo_LP.dll	machineinfo_Implant.dll	获取主机相关信息
IpConfig_LP.dll	IpConfig_Implant.dll	IP 信息获取
FileAttribs_LP.dll	FileAttribs_Implant.dll	文件属性获取
NetstatMon_LP.dll	NetstatMon_Implant.dll	网络状态获取
Dns_LP.dll	Dns_Implant.dll	DNS 设置获取
language_LP.dll	language_Implant.dll	语言信息获取
Environment_LP.dll	Environment_Implant.dll	环境变量信息获取
CheckMouse_LP.dll	CheckMouse_Implant.dll	鼠标相关检测
CheckKeyboard_LP.dll	CheckKeyboard_Implant.dll	键盘相关检测
NetBios_LP.dll	NetBios_Implant.dll	网络共享查看
NetGetDCName_LP.dll	NetGetDCName_Implant.dll	网络主机名获取
Scheduler_LP.dll	Scheduler_Implant.dll	计划任务设置
AdUser_LP.dll	AdUser_Implant.dll	添加账户
ArpScan_LP.dll	ArpScan_Implant.dll	ARP 扫描
PacketRedirect_LP.dll	PacketRedirect_Implant.dll	数据包重定向
PacketScan_LP.dll	PacketScan_Implant.dll	数据包扫描
RegKeys_LP.dll	RegKeys_Implant.dll	注册表操作
RegQuery_LP.dll	RegQuery_Implant.dll	注册表键值内容获取
procMon_LP.dll	procMon_Implant.dll	进程监控
RemoteExecute_LP.dll	RemoteExecute_Implant.dll	远程执行文件

安天 CERT 根据分析出的部分实体文件功能和文件列表进行梳理，再加上之前卡巴斯基^[7]和安天^[1]对方程式插件的分析，整理了这些功能插件在攻击过程中可能形成的组合，并绘制了“方程式组织主机作业模块积木图”。从图中可以看出攻击者通过对这些插件进行组合来完成相应的功能，这些插件体现了如下架构风格——不编写功能高度复杂的单一木马，而是把功能拆解成高度独立的小模块，这种拆解的粒度，几乎到了“原子化”的程度，即使简单如获取系统信息的操作，也把类似获取环境变量、语言集、网络状态等都作为一个独立的小模块，这将保证系统作业可以完全按需展开，从而最大化的保证作业的谨慎和静默。

从对主机安全环境的逃逸和对抗来看，这批插件的编译时间为 2007 年，从反病毒技术发展上来看，正是主机主动防御技术走入成熟的阶段。主动防御技术普遍采用行为加权的思路对未知文件进行判定，但这些完成这种“原子”操作的模块，是不会累加到阈值的。这种单独功能片段不仅在当时的情况下很难被发现，即使从现代的动静态检测角度上来看也很难被发现。每个单独功能片段不具任何明显的恶意功能，只有总调度平台将各功能插件协调使用才会组合出各种作业能力。这种作业方式，也会导致安全厂商很难获取到

完整的模块，而在没有有效 Loader 的情况下，这些模块很难在沙箱中被加载起来，从而也很难有效地进行行为分析，其比那些探测虚拟环境从而拒绝执行的木马更难以分析。

从文件名上来看，这些模块的功能规划得非常清晰。当然在实际作业中，这些 DLL 可能会以其他的一些形态表现出来，其中包括可能使用窃取的数字证书进行签名。在这种情况下，部分驱动文件的 Version 信息预计也会被定制为对应的数字证书信息，其使用的文件名，可能与其伪装的系统或应用的风格一致，或者使用类似震网^[12]、毒曲^[13]和火焰^[14]中使用的伪装成预编译或者临时文件的技巧。

表 4-3 系列 A²PT 行动中样本使用的数字签名和场景中的文件命名风格

A ² PT 事件	使用过的签名信息	命名规律
Stuxnet	JMicron Technology Corp	仿冒系统文件如：MRxCls.sys, S7HKIMDX.DLL, comspol32.ocx；按照 Windows 命名规律伪装成 oem、和 mdm 开头的 pnf 预编译文件；伪装成临时文件。
	Realtek Semiconductor Corp	
Flame	亚洲诚信数字签名测试证书	仿冒系统文件名，如：MSSECMGR.OCX, icsvntu32.ocx, FRAGWIZ.OCX
Duqu	HON HAI PRECISION INDUSTRY CO. LTD	仿冒系统文件名，如：adpu321.sys, igdkmd16b.sys, iaStor451.sys
	C-Media Electronics Incorporation	
Equation	尚未发现	仿冒系统文件名，如：mstep32.sys, DXGHL16.SYS, tdi6.sys；伪装成 Dat 文件。

当然，这些模块也可能是以采用文件不落地的方式进行投放的，其直接运行在内存中，而没有相应的文件实体。

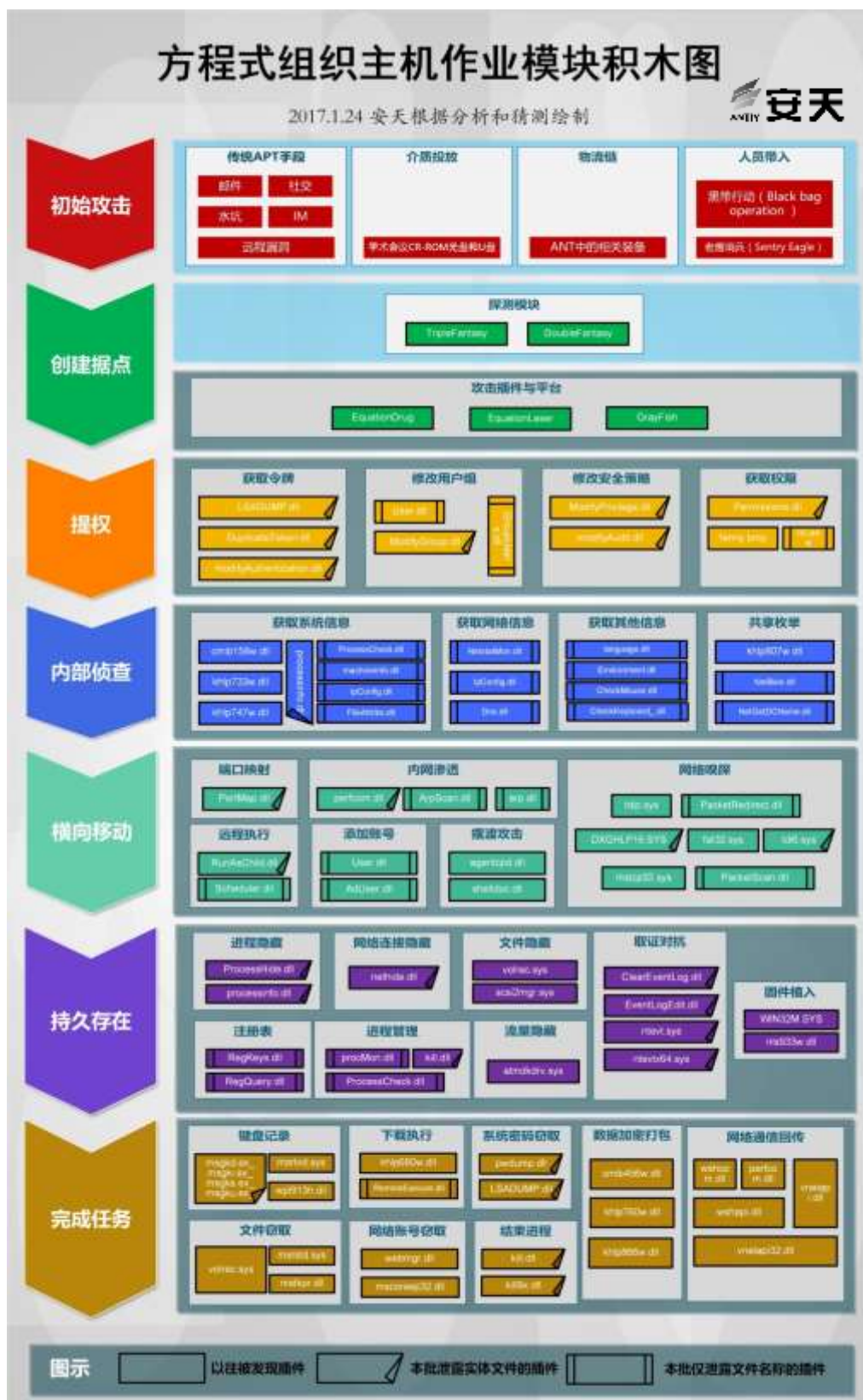


图 4-3 方程式组织主机作业模块积木图

“DanderSpritz”一词在“棱镜”事件中曾被曝光，在 ANT 中的“FIREWALK”^[16]工具中也提及到了 DNT 的“DanderSpritz”，DNT 与 ANT 同属于 NSA 的网络组织。类似这种攻击装备可被用于多种作业场景，

通过“FIREWALK”^[16]工具的网络流量采集和注入使得受害主机与攻击者的远程控制中心建立联系，使得远控变成了抵近战术作业，如，通过物流链劫持或者在内部节点上插入或替换设备，只要启动远控工具，就可以达成就近控制和人工作业相结合的攻击方式。

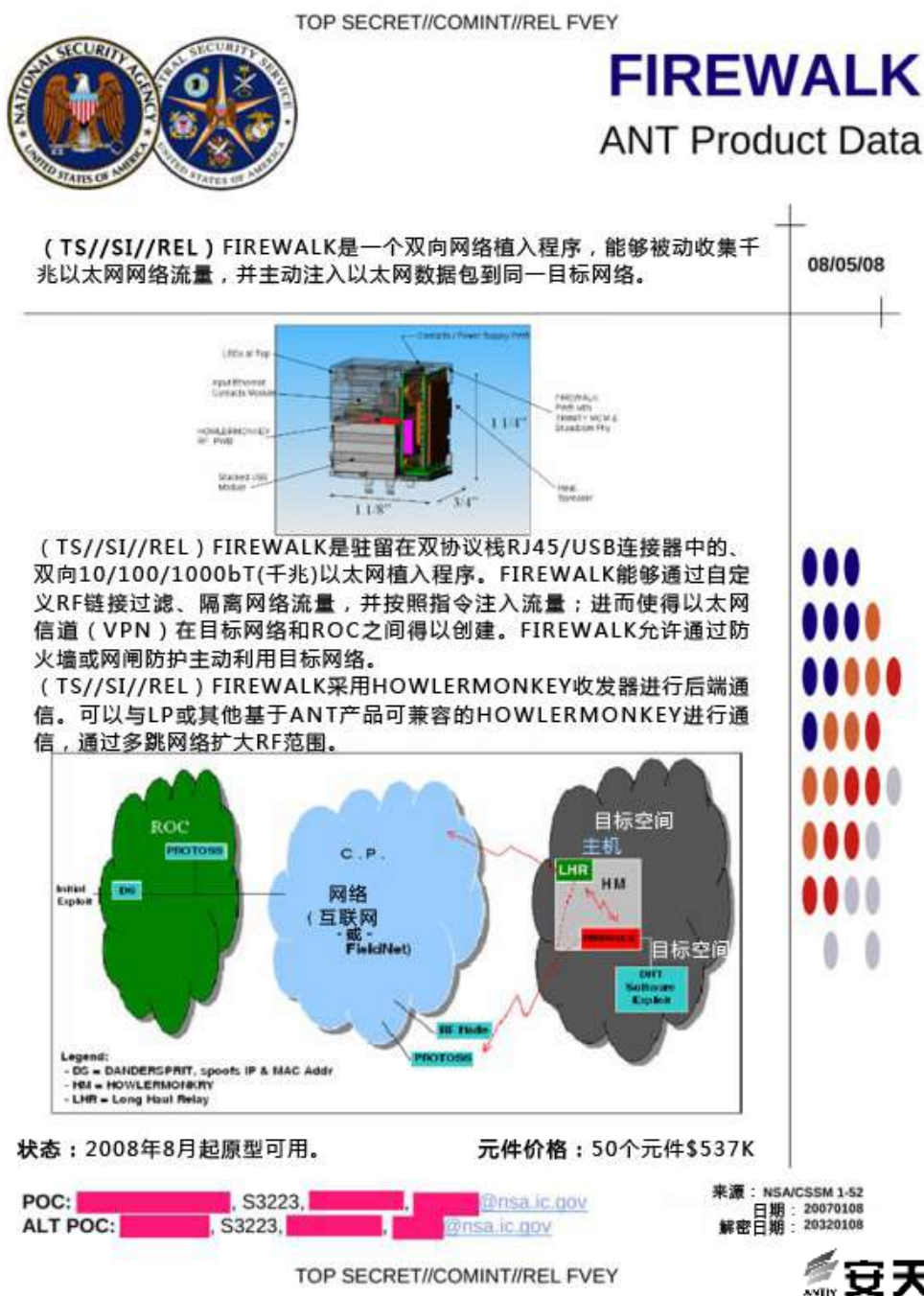


图 4-4 斯诺登曝光的 NSA-ANT 网络武器 FIREWALK (安天公益翻译小组译)

NSA-ANT 网络武器最早在 2013 年斯诺登事件中曝光，共包含 48 个攻击武器，随着事件的发酵，不断有媒体和组织对其进行曝光，安天安全分析工程师根据目前曝光的全部资料和技术分析尝试初步绘制了相关攻击装备的图谱。

NSA攻击装备体系库

(2017.1.16 安天绘制，持续整理完善中)



图 4-5 NSA-TAO 攻击装备体系（完善中）

5 部分组件与插件分析（继续完善中）

通过一段时间的跟进分析安天 CERT 发现此次曝光的插件具有模块化和反检测特点，安天 CERT 根据现有分析情况总结了这批攻击插件的三个特点：

1. 各个插件在 DllMain 函数中均不直接实现恶意行为。基于沙箱的威胁检测系统在检测 DLL 形态 PE 文件时，通常会调用 Windows API LoadLibrary() 来实现动态加载待检测对象，执行待检测对象的 DllMain 函数功能，触发待检测对象动态行为。但对于这些方程式插件，由于 DllMain 函数并不表现恶意行为（如图 5-1 所示），很容易被沙箱视作非恶意程序。


```
BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
    if ( fdwReason == 1 )
        DisableThreadLibraryCalls(hinstDLL);
    return 1;
}
```



图 5-1DllMain 函数并没有恶意功能

2. 各插件的导出函数中均不直接实现恶意功能。这些方程式插件均只提供 4 个按序号（而不是按名称）导出的函数。在其函数功能中，第 1 个导出函数负责接收调用者以特定数据结构传递的回调函数指针或参数（如图 5-2 所示）；第 2 个导出函数负责在必要释放已申请资源；第 3 个导出函数根据调用参数返回其核心功能函数指针；第 4 个导出函数负责填写调用者提供的数据结构、向调用者传递插件版本信息。除了第 4 个导出函数未对参数进行严格判断而可能因访问空指针产生异常外，各插件的导出函数均不直接实现恶意功能，基于沙箱的威胁检测系统无法通过调用各导出函数触发其恶意行为，从而将其视作非恶意程序。

```
1 int __cdecl i_1(i1_structure *a1, int a2)
2 {
3     int result; // eax@3
4
5     if ( a1 && a2 == 28 )
6     {
7         callback_1 = a1->field_1;
8         callback_2 = a1->field_2;
9         callback_3 = a1->field_3;
10        callback_4 = a1->field_4;
11        callback_5 = a1->field_5;
12        callback_6 = a1->field_6;
13        callback_7 = a1->field_7;
14        result = checkMutex() != 0;
15    }
16    else
17    {
18        result = 0;
19    }
20    return result;
21 }
```

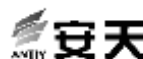


图 5-2i1 函数中的回调函数指针或参数

3. 各个插件均只实现最基本能力。这些方程式插件均只实现最基本的功能，即使分析人员掌握了插件的调用方法，传递正确的调用参数，也只能执行最基本的程序功能，并在回调函数得到程序功能的中间结果（如进程名称、模块名称、用户密码），如果不是非常有经验的分析人员，是很难将这些程序功能与正常程序的功能实现区分开。方程式攻击组织这样设计插件，除了考虑到框架的可扩展性和功能剪裁的方便性等因素之外，很可能是以此绕过某些反病毒引擎的静态检测机制。

5.1 Processinfo 插件遍历进程模块

由于这批插件的复杂性，安天 CERT 挑选了其中相对较小的文件以便于分析。通过分析发现，用于实现对指定进程的模块遍历，并调用上层模块预设的回调函数。

5.1.1 样本标签

表 5-1 样本标签

病毒名	Trojan/Win32.EquationDrug
原始文件名	processinfo_Implant9x.dll
MD5	6042EA9707316784FBC77A8B450E0991
处理器架构	X86-32
文件大小	8 KB (8,192 字节)
文件格式	BinExecute/Microsoft.DLL[:X86]
时间戳	45A40EC7->2007-01-10 05:53:11

5.1.2 主要功能

本插件提供四个基于序号导出的函数。

表 5-2 主要功能

序号	功能
1	设置上层模块回调函数，创建互斥体
2	释放资源
3	返回核心功能函数地址
4	获取插件版本信息

```

if ( a1 && a2 == 28 )
{
    dwUnk1 = *(_DWORD *)a1;
    pCallback1 = *(_DWORD *)(a1 + 4);           // callback1(DWORD, DWORD, DWORD, DWORD, DWORD);
    pCallback2 = *(_DWORD *)(a1 + 8);           // callback2();
    pCallback3 = *(int (**)(void))(a1 + 12);    // callback3();
    pCallback4 = *(int (**)(void))(a1 + 16);    // callback4();
    dwUnk2 = *(_DWORD *)(a1 + 20);
    pCallback5 = *(_DWORD *)(a1 + 24);          // callback5(DWORD);
    result = (unsigned __int8)createMutex() != 0;
}
else
{
    result = 0;
}

```

图 5-3 1 号导出函数设置上层模块回调函数

```

unsigned int __cdecl i_3(char a1)
{
    return a1 == 16 ? (unsigned int)queryProcessInfo : 0;
}

```

图 5-43 号导出函数返回核心功能函数地址

```

int __cdecl i_4(int a1)
{
    int result; // eax@1

    result = a1;
    if ( a1 )
    {
        *(_DWORD *)(a1 + 4) = 0;
        *(_DWORD *)a1 = 2;
        *(_DWORD *)(a1 + 8) = 2;
        *(_DWORD *)(a1 + 12) = 0x20000;
    }
    return result;
}

```

图 5-54 号导出函数获取插件版本信息

```

v3 = *(DWORD **)(a2 + 12);
if ( !v3 || *(_DWORD *)(a2 + 8) < 5u || (v4 = *v3) == 0 )
    v4 = GetCurrentProcessId();
hSnapshot = CreateToolhelp32Snapshot(8u, v4);
v6 = hSnapshot;
if ( hSnapshot == (HANDLE)-1 )
{
    *(_DWORD *)(errorCode + 4) = GetLastError();
    *(_DWORD *)errorCode = 1028;
    result = 1;
}
else
{
    fillStruct(&v10, (int)hSnapshot);
    v11 = 0;
    v8 = getModuleList(errorCode, v6);
    v9 = 0;
    if ( !v8 )
        v9 = 1;
    v11 = -1;
    cleanup((int)&v10);
    result = v9;
}

```

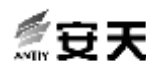


图 5-6 遍历指定进程，默认为当前进程

```

memset(&pModuleEntry, 0, 0x224u);
pModuleEntry = 548;
if ( Module32First(hSnapshot, (LPMODULEENTRY32)&pModuleEntry) )
{
    do
    {
        memset(&Dst, 0, 0x20u);
        fillZeroStruct((int)&pFileName);
        LOBYTE(v17) = 1;
        Dst = v6;
        v11 = v8;
        v12 = v7;
        getFileSHA1(fileName, &sha1);
        safeStrCpy((char **)&pFileName, fileName);
        getData((int)&data, &count, 4u);
        getData((int)&data, &Dst, 0x20u);
        v3 = (char *)sub_6800166E((int)&pFileName);
        sub_680013E0((int)&data, v3);
        LOBYTE(v17) = 0;
        sub_6800162B((int)&pFileName);
    }
    while ( Module32Next(hSnapshot, (LPMODULEENTRY32)&pModuleEntry) );
    v2 = 1;
}
else
{
    *(_DWORD *)a1 = 1030;
    *(_DWORD *)a1 + 4 = 0;
}

```

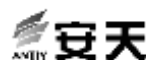


图 5-7 遍历指定进程模块，计算模块对应文件 HASH（SHA1）

5.2 kill_Implant 插件杀进程模块

该模块是另一个相对较小的文件，安天 CERT 通过分析发现，该插件主要功能为根据传入的进程 ID 来结束对应进程。

5.2.1 样本标签

表 5-3 样本标签

病毒名	Trojan/Win32.EquationDrug
原始文件名	kill_Implant.dll
MD5	BDD2B462E050EF2FA7778526EA4A2A58
处理器架构	X86-32
文件大小	21 KB(21,504 字节)
文件格式	BinExecute/Microsoft.DLL[:X86]
时间戳	45A40616->2007-01-10 05:16:06

5.2.2 主要功能

模块调用者传递进来进程 ID，该模块利用函数 `OpenProcess` 获取句柄，再利用函数 `TerminateProcess` 结束对应进程。

```
hProcess = OpenProcess(1u, 0, *v3);
v5 = GetLastError();
if ( hProcess || *((_BYTE *)v3 + 4) && (v5 = sub_6800118F(*v3, 1, &hProcess), hProcess) )
{
    sub_68004135(hProcess);
    v10 = 0;
    if ( TerminateProcess(hProcess, 0) )
    {
        v4 = 0;
    }
}
```

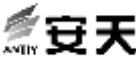


图 5-8 结束进程

5.3 GROK 键盘与剪贴版记录器驱动

本次泄露的文件除 DLL 插件外还有一些 EXE 格式，安天 CERT 发现其中几个 EXE 文件与之前方程式平台中的 GROK 组件相同，本次曝光的版本为 1.2.0.1，均可以从资源段中解密并释放键盘与剪贴版记录器驱动 `msrtdv.sys`。

5.3.1 样本标签

表 5-4 样本标签

病毒名	Trojan/Win32.EquationDrug
原始文件名	msrtdv.sys
MD5	6A4461AF87371B89D240A34846A7BC64
处理器架构	X86-32
文件大小	36.3 KB (37,248 字节)
文件格式	BinExecute/Microsoft.SYS[:X86]
时间戳	0x4B7F1480—>2010-02-20 06:45:20

该恶意代码样本是键盘记录器及剪贴板监视工具，在之前友商报告中曾经提到过有相似功能的恶意代码，下面对其相似之处进行对比。

5.3.2 版本信息

样本包含版本信息，文件版本为 5.1.1364.6430，源文件名为 msrtdv.sys，文件描述为 MSRTdvinterface driver。其中文件版本低于之前已经曝光的版本 5.3.1365.2180，源文件名与文件描述的不同在于将两个字母“d”和“v”的位置互换，一个是“mstrdv.sys”，另一个是“msrtvd.sys”。

本次泄露的版本		之前曝光的版本
property	value	value
file-type	device-driver	device-driver
file-subtype	System Driver	System Driver
date	n/a	n/a
language	English United States	English United States
code-page	Unicode UTF-16, little endian	Unicode UTF-16, little endian
CompanyName	Microsoft Corporation	Microsoft Corporation
FileDescription	MSRTdv interface driver	MSRTvd interface driver
FileVersion	5.1.1364.6430	5.3.1365.2180
InternalName	msrtdv.sys	msrtvd.sys
LegalCopyright	© Microsoft Corporation. All rights reserved.	© Microsoft Corporation. All rights reserved.
OriginalFilename	msrtdv.sys	msrtvd.sys
ProductName	Microsoft® Windows® Operating System	Microsoft® Windows® Operating System
ProductVersion	5.1.1364.6430	5.3.1365.2180

图 5-9 本次泄露版本与之前曝光版本的版本信息

5.3.3 主要功能

两个不同版本的样本其主要功能相同，通过给转储程序建立专用的进程来汇集所收集的数据，每隔 30 分钟，将结果压缩到文件"%TEMP%\tm154o.da"。之前曝光的版本中，包含多个 IoControlCode，分别对应不同的功能。

```

if ( *(u3 + 12) == 0x22002C )           // 启动转储程序线程
{
    u8 = sub_11760(sub_10FDE, -1);
    goto LABEL_31;
}
if ( *(u3 + 12) == 0x220030 )           // 结束转储程序线程
{
    sub_10FDE(0, 0);
    dword_177E4 = 1;
    u8 = sub_117B6();
}
if ( *(u3 + 12) == 0x220034 )           // 检查驱动程序是否具有新数据进行转储
{
    u5 = dword_177D8;
    if ( !dword_177D8 )
    {
        u8 = 0x80000022;
        goto LABEL_33;
    }
}
if ( *(u3 + 12) == 0x220038 )           // 设置外部事件示意转储数据可用性
{
    if ( *(u3 + 8) != 8 || !(u2 + 12) )
    {
        u8 = -1073741823;
        goto LABEL_33;
    }
    u10 = sub_10C5C();
}
if ( *(u3 + 12) == 0x22003C )           // 重新启动转储程序线程
{
    sub_10FDE(0, 0);
    u8 = sub_117C6();
    goto LABEL_33;
}
if ( *(u3 + 12) == 2228288 )           // 获取有效数据的大小

```

图 5-10 之前曝光版本的主要功能代码

而本次泄露的样本中，IoControlCode 虽然只有 0x22002C，但一些主要功能仍然存在，可以通过反编译后的代码看出它们的相同之处。

```

if ( *(v8 + 12) == 0x22002C )
{
    v10 = wcslen(&word_1136E);
    v3 = 2 * (1 - v10 + wcslen(SourceString));
    if ( v3 <= *(v8 + 4) ) // 检查驱动程序是否具有新数据进行转储
    {
        qmemcpy(v6, SourceString, 0x104u);
        v5[wcslen(v6)] = 100;
        v9 = sub_111262(v6);
        if ( v9 >= 0 )
        {
            qmemcpy(*(a2 + 12), &v6[v10], v3);
            *(v8 + 4) = v3;
            *(a2 + 28) = v3;
        }
    }
}
else // 结束转储程序线程
{
    if ( *v2 != 16 )
        goto LABEL_10;
    InterlockedDecrement(v3);
    v4 = sub_110D8(a1);
}

int v1; // esi@2
__int16 v3[4]; // [sp+0h] [bp-210h]@3
wchar_t v4; // [sp+8h] [bp-208h]@3

sub_117D4();
if ( sub_10486() )
{

```

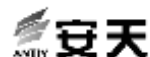


图 5-11 之前曝光版本的主要功能代码

```

if ( *(v8 + 12) == 0x22002C )
{
    v10 = wcslen(&word_1136E);
    v3 = 2 * (1 - v10 + wcslen(SourceString));
    if ( v3 <= *(v8 + 4) ) // 检查驱动程序是否具有新数据进行转储
    {
        qmemcpy(v6, SourceString, 0x104u);
        v5[wcslen(v6)] = 100;
        v9 = sub_111262(v6);
        if ( v9 >= 0 )
        {
            qmemcpy(*(a2 + 12), &v6[v10], v3);
            *(v8 + 4) = v3;
            *(a2 + 28) = v3;
        }
    }
}
else // 结束转储程序线程
{
    if ( *v2 != 16 )
        goto LABEL_10;
    InterlockedDecrement(v3);
    v4 = sub_110D8(a1);
}

int v1; // esi@2
__int16 v3[4]; // [sp+0h] [bp-210h]@3
wchar_t v4; // [sp+8h] [bp-208h]@3

sub_117D4();
if ( sub_10486() )
{

```



图 5-12 本次泄露版本的主要功能代码

从以上分析比较中可以发现，本次泄露的恶意代码样本应为较低版本，版本信息低于之前卡巴斯基与安天分析曝光的版本，功能也弱于相关版本。在影子经纪人泄露出的文件 DanderSpritz_All_Find.txt 中，GROK 的版本号也清楚的说明了这个问题，“影子经纪人”所释放出的只是 GROK 组件的低版本部分文件。但这批文件信息的丰富程度，则是将“千年暗室”打开了一个难得的缝隙。

```
./Resources/GROK/1.2.0.1/Uploads/msgkd.ex_  
./Resources/GROK/1.2.0.1/Uploads/msgki.ex_  
./Resources/GROK/1.2.0.1/Uploads/msgks.ex_  
./Resources/GROK/1.2.0.1/Uploads/msgku.ex_  
./Resources/GROK/2.1.3.1  
./Resources/GROK/2.1.3.1/Offline  
./Resources/GROK/2.1.3.1/Offline/GkDecoder.exe  
./Resources/GROK/2.1.3.1/Offline/UtilPaku.dll  
./Resources/GROK/2.1.3.1/Offline/Xml4_0u.dll
```

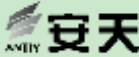


图 5-13GROK 组件的不同版本号

6 小结

此次“影子经纪人”释放的 Equation Group 中的 61 个文件，对于全球网络安全研究者分析厘清 EQUATION 相关攻击平台的组成和架构有很大帮助。特别是能够观察其恶意代码的 Debug 版本，这在常规与超级攻击组织的对抗中是很难想象的，这是一次难得从“内部”观察发动方程式组织的机会。经过初步打通和分析相关曝光信息，安天 CERT 看到、分析和梳理了该攻击平台的更多信息，包括如数百个攻击插件以及“DanderSpritz”攻击平台。

安天 CERT 分析相关文件后，判断其中部分组件与之前曝光的 GROK 组件为同类样本，而这些组件均为早期的低版本。另外，安天 CERT 的分析结果也表明“DanderSpritz”与 Equation Drug 使用了相同的组件和架构设计，“DanderSpritz”可能就是方程式组织使用的 Equation Drug 攻击平台，而其模块“原子化”的设计思路，让更多人可以看到该方程式组织支撑体系的庞大精密，作业过程的严密谨慎，以及其在武器研发使用中，绕过安全防御手段异常丰富的经验。

五年前，在安天展开针对 Flame（火焰）蠕虫的马拉松分析中，有专家曾提醒我们不要“只见树叶，不见森林”，这让安天的安全工程师们深刻地反思了传统分析工程师“视野从入口点开始”的局限性，从那时开始尝试建立从微观见宏观的分析视野。安天 CERT 的安全工程师们通过本次分析，发现自己依然在迷宫中挣扎——或许这就是面对超级攻击者时，安全分析团队面临的分析常态。

过去的四年，针对方程式组织的持续跟踪分析，是安天了解最高级别攻击者（即 A²PT——高级的 APT）的极为难得的经历。深入研究这种具有超级成本支撑和先进理念引领的超级攻击者，对于改善和增强安天

探海、智甲、追影等高级威胁检测和防御产品的防御能力也非常关键。安天也在深入思考和探索面对行业和地域的大规模态势感知系统，即达成“以资产防护为核心”的有效能力，尤其是面对海量事件锁定关键威胁和高级攻击者的能力。但对于应对 A²PT 攻击者来说，无论是有效改善防御，还是进行更为全面深入系统的分析，都不是一家安全企业能够独立承载的，此中还需要更多协同和接力式分析，而不是重复“发明轮子”。正是基于这种共同认知，在不久之前的第四届安天网络安全冬训营上，安天和 360 企业安全等安全企业向部分与会专家介绍了能力型安全厂商分析成果互认的部分尝试。唯有中国的机构用户和能力型安全厂商形成一个积极互动的体系，才能更好的防御来自各方面的威胁。

我们警惕，但并不恐惧。对于一场防御战而言，除了扎实的架构、防御和分析工作之外，必胜的信念是一个最大的前提。

无形者未必无影，安天追影，画影图形。

附录一：参考资料

[1] 安天《修改硬盘固件的木马探索方程式（EQUATION）组织的攻击组件》

http://www.antiy.com/response/EQUATION_ANTIY_REPORT.html

[2] 安天《方程式（EQUATION）部分组件中的加密技巧分析》

http://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html

[3] 安天《从“方程式”到“方程组” EQUATION 攻击组织高级恶意代码的全平台能力解析》

<http://www.antiy.com/response/EQUATIONS/EQUATIONS.html>

[4] TheShadowBrokers closed, going dark

<https://onlyzero.net/theshadowbrokers.bit/post/messagefinale/>

[5] Stolen NSA "Windows Hacking Tools" Now Up For Sale!

<http://thehackernews.com/2017/01/nsa-windows-hacking-tools.html>

[6] Kaspersky: Equation: The Death Star of Malware Galaxy

<http://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/>

[7] Kaspersky: Inside the EquationDrug Espionage Platform

<https://securelist.com/blog/research/69203/inside-the-equationdrug-espionage-platform/>

[8] Equation Group Cyber Weapons Auction - Invitation

<https://github.com/theshadowbrokers/EQGRP-AUCTION>

[9] The Equation giveaway

<https://securelist.com/blog/incidents/75812/the-equation-giveaway/>

[10] I just published “TheShadowBrokers Message #3”

<https://medium.com/@shadowbrokersss/theshadowbrokers-message-3-af1b181b481>

[11] Shadow Brokers reveals list of Servers Hacked by the NSA

<http://thehackernews.com/2016/10/nsa-shadow-brokers-hacking.html>

[12] 安天《对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告》

http://www.antiy.com/response/stuxnet/Report_on_the_Worm_Stuxnet_Attack.html

[13] 《管中窥豹——Stuxnet、Duqu 和 Flame 的分析碎片与反思》

http://www.antiy.com/resources/Analysis_and_Introspection_of_Stuxnet_Duqu_and_Flame.pdf

[14] Flame 蠕虫样本集分析报告

http://www.antiy.com/response/flame/Analysis_on_the_Flame.html

[15] ANTProductData2013

<https://search.edwardsnowden.com/docs/ANTProductData2013-12-30nsadocs>

[16] Kaspersky: A Fanny Equation: "I am your father, Stuxnet"

<http://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/>

[17] Kaspersky: Equation Group: from Houston with love

<http://securelist.com/blog/research/68877/equation-group-from-houston-with-love/>

[18] Kaspersky: Equation_group_questions_and_answers

https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

[19] Kaspersky: The Equation giveaway

<https://securelist.com/blog/incidents/75812/the-equation-giveaway/>

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为以安天实验室为总部，以企业安全公司、移动安全公司为两翼的集团化安全企业。安天始终坚持以安全保障用户价值为企业信仰，崇尚自主研发创新，在安全检测引擎、移动安全、网络协议分析还原、动态分析、终端防护、虚拟化安全等方面形成了全能力链布局。安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展工程师团队作业能力、缩短产品响应周期。结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了应对高级持续性威胁（APT）和面向大规模网络与关键基础设施的态势感知与监控预警解决方案。

全球超过三十家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近两亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

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，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码 II、口令蠕虫、震网、破壳、沙虫、方程式等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

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问：<http://www.antiy.cn>