网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

震网与SWIFT事件回顾

从威胁框架看超高能力网空威胁行为体的两种作业模式

安天应急响应中心

威胁框架：认知与实践

寒夜遠征

寒夜迷途

CONTENTS

目 录

01 震网事件回顾与历史疑惑分析

02 中东SWIFT服务商被入侵复盘

03 体系化支撑下的集成化武器作业与远程推进式作业

寒夜遠征

威胁框架：认知与实践

01 震网事件回顾与历史疑惑分析

震网事件的九年再复盘与思考

扫码阅读安天原创报告

2010年7月

“震网”（Stuxnet）蠕虫攻击事件浮出水面，引发了国际主流安全厂商和安全研究者的全面关注，这是一起经过长期规划准备和入侵潜伏作业；借助高度复杂的恶意代码和多个零日漏洞作为攻击武器；以铀离心机为攻击目标；以造成超压导致离心机批量损坏和改变离心机转数导致铀无法满足武器要求为致效机理，以阻断伊朗核武器进程为目的的攻击。

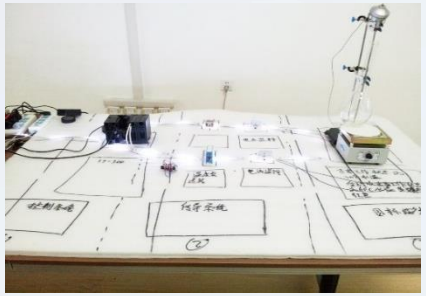
2019年9月30日

安天CERT对震网事件重新复盘，绘制整体运行框架、进行威胁框架下的映射解读、公布USB摆渡机理、分析扩散式传播原因、基于Tilded框架与Flamer框架的关联梳理震网、毒曲、火焰、高斯、Fanny、Flowershop的同源关系，分析震网样本数量众多的原因。思考检测引擎与威胁情报面临的挑战。

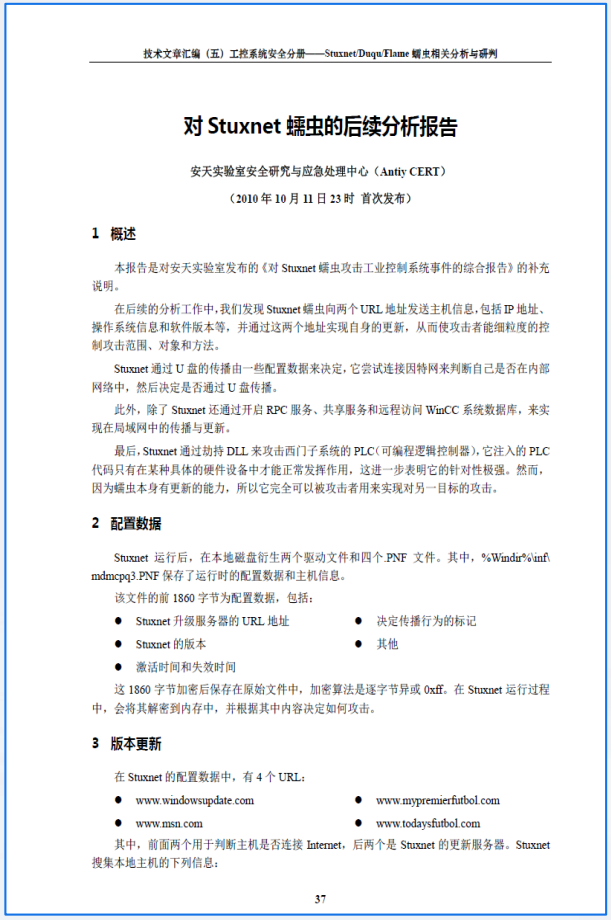
2010~2012年安天的部分分析工作

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
WINCC后发生了什么?	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。



制作工控系统安全威胁实景模拟系统一套



技术文章汇编（五）工控系统安全分册——Stuxnet/Duqu/Flame 蠕虫相关分析与研判

对 Stuxnet 蠕虫的后续分析报告

安天实验室安全研究与应急处理中心（Antiy CERT）

（2010 年 10 月 11 日 23 时 首次发布）

1 概述

本报告是对安天实验室发布的《对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告》的补充说明。

在后续的分析工作中，我们发现 Stuxnet 蠕虫向两个 URL 地址发送主机信息，包括 IP 地址、操作系统信息和软件版本等，并通过这两个地址实现自身的更新，从而使攻击者能细粒度的控制攻击范围、对象和方法。

Stuxnet 通过 U 盘的传播由一些配置数据来决定，它尝试连接因特网来判断自己是否在内部网络中，然后决定是否通过 U 盘传播。

此外，除了 Stuxnet 还通过开启 RPC 服务、共享服务和远程访问 WinCC 系统数据库，来实现在局域网中的传播与更新。

最后，Stuxnet 通过劫持 DLL 来攻击西门子系统的 PLC（可编程逻辑控制器），它注入的 PLC 代码只有在某种具体的硬件设备中才能正常发挥作用，这进一步表明它的针对性极强。然而，因为蠕虫本身有更新的能力，所以它完全可以被攻击者用来实现对另一目标的攻击。

2 配置数据

Stuxnet 运行后，在本地磁盘衍生两个驱动文件和四个.PNF 文件。其中，%Windir%\inf\mdmcpq3.PNF 保存了运行时的配置数据和主机信息。

该文件的前 1860 字节为配置数据，包括：

- Stuxnet 升级服务器的 URL 地址
- Stuxnet 的版本
- 激活时间和失效时间
- 决定传播行为的标记
- 其他

这 1860 字节加密后保存在原始文件中，加密算法是逐字节异或 0xff。在 Stuxnet 运行过程中，会将其解密到内存中，并根据其中内容决定如何攻击。

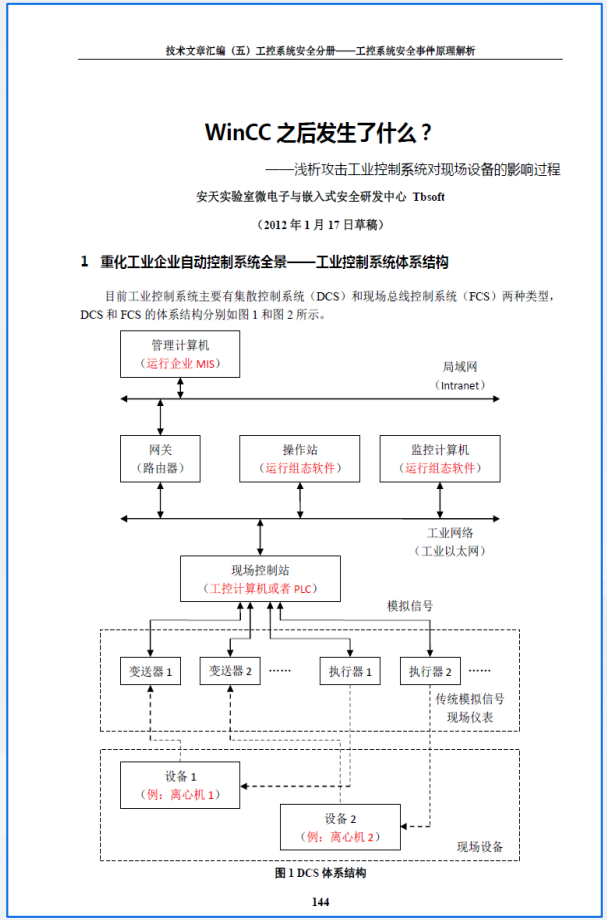
3 版本更新

在 Stuxnet 的配置数据中，有 4 个 URL：

- www.windowsupdate.com
- www.msn.com
- www.mypremierfutbol.com
- www.todaysfutbol.com

其中，前面两个用于判断主机是否连接 Internet，后两个是 Stuxnet 的更新服务器。Stuxnet 搜集本地主机的下列信息：

37



技术文章汇编（五）工控系统安全分册——工控系统安全事件原理解析

WinCC 之后发生了什么？

——浅析攻击工业控制系统对现场设备的影响过程

安天实验室微电子与嵌入式安全研发中心 Tbsoft

（2012 年 1 月 17 日草稿）

1 重化工业企业自动控制系统全景——工业控制系统体系结构

目前工业控制系统主要有集散控制系统（DCS）和现场总线控制系统（FCS）两种类型，DCS 和 FCS 的体系结构分别如图 1 和图 2 所示。

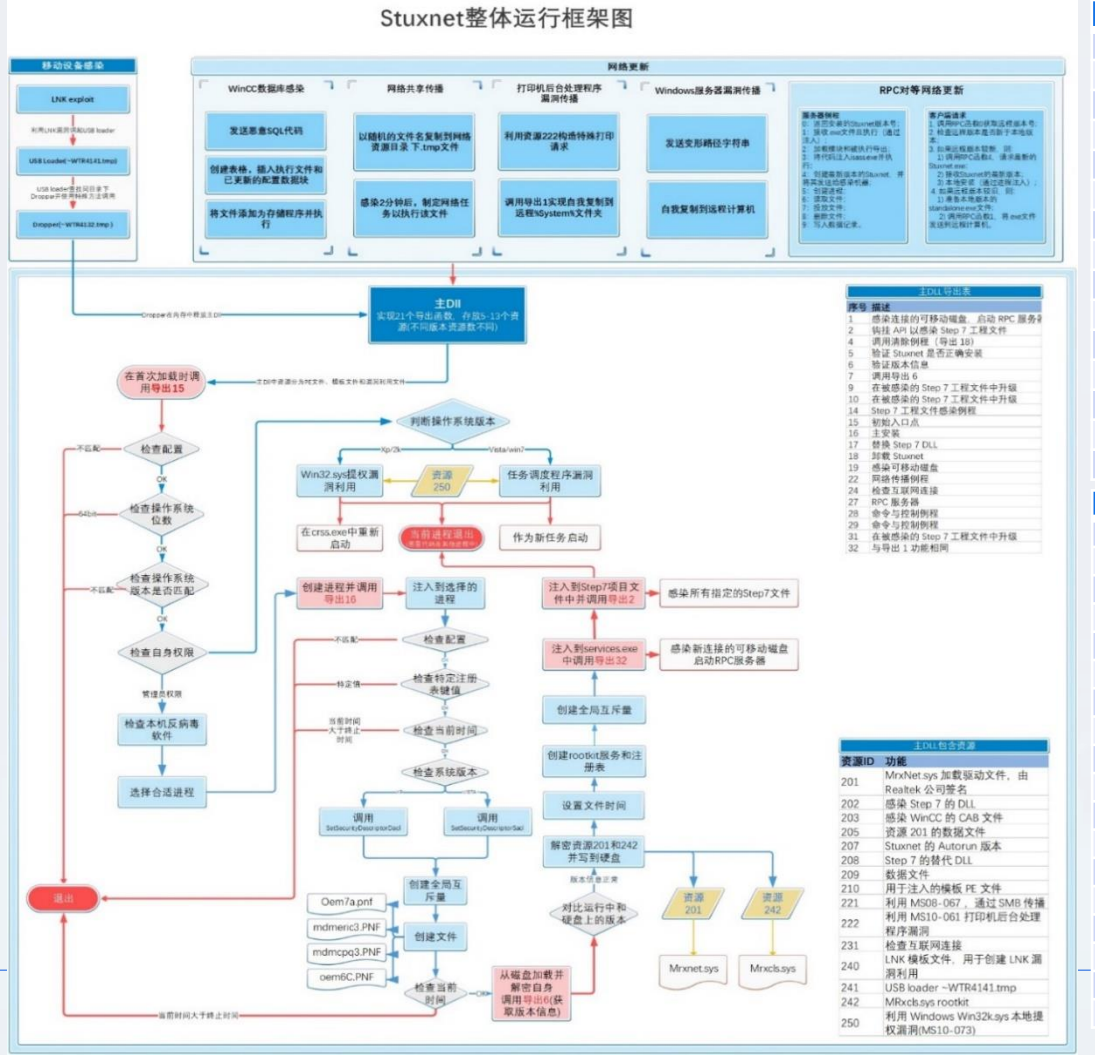
图 1 DCS 体系结构

144

震网事件时间轴

图例
攻击方
受害方
分析防御方
发布补丁方
2010/7/23
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
2010/7/20
Symantec检测到C&C流量
Kaspersky博文介绍Stuxnet的证书
Symantec博文介绍Stuxnet传播方法
2010/7/19
Kaspersky博文介绍LNK漏洞原理
西门子报告Stuxnet攻击其SCADA系统
2010/7/16
微软发布LNK漏洞预警
Symantec博文介绍Stuxnet基本情况
2010/7/15
Kaspersky三篇博文讨论LNK漏洞和签名驱动
安天捕获第一个样本，并添加检测规则
2010/7/13
Symantec检测样本为W32.Temphid
2010/6/17
Virusblokada上报样本，"震网"病毒首次被发现，它被称为有史以来最复杂的网络武器
2009/7/7
Control-Gostar jahed Commpany 公司
位于伊朗，主要是做工业自动化
2009/7/7
Neda Industrial Group 公司
位于伊朗，为水电站、水泥、以及石油、天然气及石化领域，提供工业自动化服务
2009/6/28
Behpajooh Co. Elec & Comp. Engineering公司
位于伊朗-伊斯法罕，主要开发工业自动化系统
2009/6/23
FOOLAD Technic Engineering Co(FIECO)公司
位于伊朗，主要为伊朗工业设施生产自动化系统
2008/10/23
微软公布了 MS08-067，这款补丁可以修补Windows Server服务RPC请求缓冲区溢出漏洞
2010/11/16
Symantec发布博文，称Stuxnet的攻击目标是伊朗某核电站中轴的浓缩设施
2010/10/11
安天补充了一篇后续报告
2010/9/30
Symantec在VB大会上演示PLC系统
2010/9/27
安天发布第一版分析报告
2010/9/26
Kaspersky发布系列博文Myrtus and Guava，介绍与伊朗的关系
Symantec发布博文，介绍Stuxnet感染Step7工程的方法
2010/9/21
Symantec发表博文介绍Stuxnet感染PLC的过程
2010/8/18
安天发布一篇样本分析报告
2010/8/6
Symantec发布博文称其是第一个针对工控系统的rootkit
2010/10/12
微软公布了MS10-073，Windows 内核模式驱动程序中的漏洞可能允许特权提升
2010/9/14
微软公布了MS10-061（CVE-2010-2729）这款补丁可以修补打印后台程序漏洞。
2010/8/2
微软公布MS10-046（CVE-2010-2568），这款补丁可以修补Windows Shell快捷方式的漏洞
2011/12/28
Kaspersky公布Stuxnet与Duqu的关联分析
2011/2
Kaspersky公布对Stuxnet时间戳的关联分析
2012/1/23
安天完成关于WINCC对轴浓缩具体影响的有关分析
安天完成Suxnet与Duqu的同源性分析并发布报告
2003年
2005年
2006年
2008年
2009年
2010年
2011年
2012年
2003/12/11
208.res最早二进制编译时间戳
2005/11/3
震网0.500版本，C&C服务器注册时间
2005/11/15
提交到公共扫描服务的日期
2006/5/22
231.res最早二进制编译时间戳
2009/1/2
201.res,最早二进制编译时间戳
2009/2/5
207.res最早二进制编译时间戳
2009/3/7
221.res最早二进制编译时间戳
222.res最早二进制编译时间戳
2009/6/4
震网0.500版本，感染停止日期
2009/6/12
震网1.001版本，二进制编译时间戳
2009/6/22
202.res最早二进制编译时间戳
210.res最早二进制编译时间戳
2010/1/25
242.res最早二进制编译时间戳
2010/2/1
250.res最早二进制编译时间戳
2010/2/3
241.res最早二进制编译时间戳
2010/3/1
震网1.100版本，二进制编译时间戳
2010/4/14
震网1.101版本，二进制编译时间戳
2010/7/31
震网1.110版本，U盘终止感染时间
2010/8/31
震网1.110版本，U盘终止感染时间
2010/12/31
震网1.100版本，U盘终止感染时间
2010/5/11
Kala Electric 公司
位于伊朗，是铀浓缩离心机设备IR-1最主要的供应商
2010/4/24
Mobarakeh Steel Company(MSC)公司
位于伊朗，是伊朗最大的钢铁制造商，伊朗经营规模最大的工业园区之一
2012/6/24
震网1.x版本感染的截止日期
安天

Stuxnet Dropper整体运行流程和资源、落地文件列表



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

Stuxnet Dropper资源列表

落地文件主要名称	文件功能/资源ID
~WTR4141.tmp	usb loader
~DF540C.tmp	状态标记文件
~wtr4132.tmp	USB感染中的dropper名
DEFRAG[RANDLNT].tmp	共享感染中的dropper名
Oem7a.pnf	加密的主dll
mdmeric3.PNF	90字节的数据文件
mdmcpq3.PNF	Stuxnet配置文件
oem6C.PNF	日志
MrxCls.sys	资源242
MrxNet.sys	资源201
s7otbxdx.dll	被替换的Step7文件
s7hkimdb.dll	资源202（stuxnet loader）
cc_tlg7.sav	CAB文件 包 含一个加载和执行Stuxnet的DLL
winmic.fts	资源209（数据文件）
winsta.exe	利用打印机漏洞传播时释放的可执行文件版Stuxnet
sysnullevnt.mof	托管对象格式文件
~WTR4141.tmp	usb loader
~DF540C.tmp	状态标记文件

Stuxnet落地文件列表

通过网空威胁框架分析“震网”事件

Administration（行动管理与资源保障）			Preparation（目标勘察与环境整备）		Engagement（接触目标与进攻突防）		Presence（持久化驻留潜伏）						Effect（致效能力运用）					Ongoing Processes（全程持续支撑作业）			
规划	资源开发	研究	侦察	环境预置	投递	利用	执行	内部侦察	提权	凭证访问	横向移动	持久化	监控	渗出	修改	拒绝	破坏	分析、评估、反馈	命令与控制	规避	
分析行动	获取行动所需基础设施	收集信息	执行社会工程学	应用数据文件中添加可利用点	无线接入	滥用协议	创建计划任务	枚举账户和权限	利用应用程序漏洞	添加或修改凭证	利用对等网络	创建新服务	激活记录	收集串扰	修改数据	破坏文件或应用程序	磁盘/操作系统变砖（全部删除）	使用基础设施	向中点发送信标	直接访问磁盘	删除日志数据
确定战略和目标	建立联盟和伙伴关系	确定能力差距	收集凭证	分配行动所需基础设施	改变通信路径	访问虚拟内存	通过服务控制器执行	枚举文件系统	利用固件漏洞	执行社会工程学	远程登录	创建计划任务	被动收集	从本地系统收集	修改进程结果	降低性能	损坏磁盘/操作系统（部分删除）	实施效果评估	建立对等网络	规避数据大小限制	删除toolkit
发布行动指令	创建僵尸网络	确定信息差距	识别串扰	建立跳板	供应链/受信源入侵	执行社会工程学	通过第三方软件执行	枚举本地网络连接	利用操作系统漏洞	破解密码	利用密码哈希认证	编辑boot记录	为其他行动创造条件	从网络资源收集	造成物理影响	中断/拒绝服务	删除数据	优化潜在受害者	中继通信	阻止主机信标上传	为恶意内容签名
制定行动计划	能力开发		测绘可访问网络	建立物理抵近点	可移动介质连接	破解加密	注入进程	枚举本地网络设置	注入进程	转储凭证	利用ticket认证	修改文件类型关联	键盘记录	压缩数据	修改机器间通信	加密数据使其不可用	破坏硬件		发送命令	降级安全产品	将文件存储在非常规的位置
获准执行行动	获得资金		扫描设备	网站植入或预埋	异常网络设备连接	利用固件漏洞	利用授权用户	枚举操作系统和软件	利用辅助功能	劫持活动的凭证	通过可移动介质复制	使用登录脚本	保持访问	泄露数据或信息	更改系统进程的运行状态				利用僵尸网络	延迟活动	根据环境调整行为
选择目标受害者	供应链 预置		爬取网站	预置载荷	通过网站感染	利用本地应用程序漏洞	替换现有二进制文件	枚举进程	利用合法凭证	定位凭证	污染共享内容	利用路径顺序执行	屏幕截屏	将数据存储到指定位置	篡改网站				利用链式协议	采用反取证措施	利用签名内容
	人员和培训资源		选择潜在受害者		注入数据库命令	利用操作系统漏洞	运行shell命令	枚举窗口		键盘记录	利用应用程序部署软件	修改BIOS		运行收集脚本	破解加密				利用对等连接	采用反逆向工程措施	
			调查设备		利用设备交换	利用远程应用程序漏洞	运行无文件载荷	测绘可访问网络			利用远程服务	修改配置用于启动		通过C2信道发送					利用远程shell	使用rootkit	
			利用社交媒体		发送恶意邮件	利用弱访问控制	利用解释脚本	扫描连接的设备			写入远程文件共享	修改现有服务		通过非C2信道发送					利用可移动介质	编码数据	
					借助公共网络基础设施传输	劫持	利用系统接口	嗅探网络			写入共享webroot目录	修改链接		通过其他网络介质发送						加密数据	
					利用CDS或MLS传输	冒充/欺骗用户	利用远程服务					修改服务配置		节流数据						仿冒合法文件	
					利用聊天服务	零日漏洞利用	通过受信应用执行非受信代码					替换服务二进制文件		通过物理方法传输						操纵受信进程	
					利用受感染主机	漏洞利用工具包	写入磁盘					设置为启动时加载		利用CDS或MLS传输						仿冒合法流量	
					利用合法远程访问	利用受信关系						利用库搜索劫持								修改恶意代码以规避检测	
					利用物理网桥	重放攻击														混淆数据	

确定使用的攻击手段

推测使用的攻击手段

震网事件中涉及的类别与具体动作

威胁框架类别	威胁框架动作	具体行为
Administration（行动管理与资源保障）	规划	可能存在对行动过程分析；在发起攻击前可能会先确定战略与目标、预先制定行动计划、选择目标受害者和获得执行行动的批准；
	资源开发	在行动前，搭建模拟靶场环境进行测试；在行动前可能会获取行动需要的基础设施、资金、联盟和伙伴，并对相关人员进行培训；
	研究	可能会存在对目标进行收集信息，研究目标网络能力；
Preparation（目标勘察与环境整备）	侦察	可能会选择潜在受害者调查网络环境与设备；
	环境预置	应用数据文件中添加可利用点；分配行动所需基础设施；可能会对目标进行预制载荷；
Engagement（接触目标与进攻突防）	投递	通过可移动介质投递载荷；利用漏洞投递载荷；利用受感染主机投递载荷；通过硬编码数据库服务器密码感染WinCC机器；可能会通过对目标供应链/授信源入侵；
	利用	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）；内核模式驱动程序漏洞（MS10-073）；任务计划程序程序漏洞（MS10-092）；
Presence（持久化驻留潜伏）	执行	注入lsass.exe与csrss.exe等系统进程；已特殊方式注入自身；替换西门子 step7驱动文件；运行无文件载荷；使用KERNEL32.DLL.ASLR.XXXX这样的DLLName调用LoadLibraryA以加载主DLL文件；利用远程服务；写入多个PNF文件；
	内部侦察	枚举账户和权限；检测安全产品；通过注册表查找特定键；枚举进程；扫描连接的移动设备；
	提权	快捷方式文件解析漏洞；RPC远程执行漏洞；打印机后台程序服务漏洞；Windows Win32K.sys本地提权（MS10-073）；
	凭证访问	转储凭证、定位凭证；
	横向移动	利用对等网络；利用密码哈希认证；通过利用一个漏洞，允许自动执行可移动驱动器；通过网络共享在远程计算机中复制和执行其本身；写入远程文件共享；通过硬编码数据库服务器密码感染WinCC机器；
	持久化	MrxCls.sys驱动文件会注册成为启动服务；创建新服务；修改服务配置；利用库搜索劫持；
Effect（致效能力运用）	监控	将信息记录到oem6c.pnf文件中；监控插入的USB设备；
	渗出	泄露数据或信息；将数据存储到指定位置；通过HTTP向攻击者发送被感染机器的基本信息；
	修改	在PLC上隐藏修订的代码，基本上是PLC的rootkit；修改进程结果；通过修改可编程逻辑控制器代码重新编程工业控制系统；修改机器间通信；
	破坏	破坏工业控制系统离心机；
Ongoing Processes（全程持续支撑作业）	分析、评估、反馈	可能存在对目标的影响进行评估；
	命令与控制	建立对等网络；通过HTTP向攻击者发送被感染机器的基本信息；利用对等连接；通过RPC对等网络更新；检查网络连接；通过命令和控件响应执行加密二进制代码；
	规避	采用反取证措施；采用反逆向工程措施；使用rootkit；编码数据；加密配制和附加数据；JMicron和Realtek签署的数字签名证书；操纵受信进程；修改恶意代码以规避检测、混淆数据；根据配置文件调整行为；

0.5和1.X版本技术细节全面对比

版本	时间	说明	漏洞利用情况	传播技术的演变	平台的演变	攻击策略的演变
0.500	2005/11/3	C&C 服务器注册	CVE-2012-3015 Step7 安全库加载	Autorun.inf 通过感染Step7项目文件 通过USB执行Step7 通过mailslot更新对等网络	基于Flamer平台	针对S7-400（417）PLCs的完整的代码序列（在铀浓缩过程中修改级联保护系统阀门操作）
0.500	2005/11/15	提交到公共扫描服务的日期				
0.500	2009/6/4	感染停止日期				
1.001	2009/6/12	二进制编译时间戳更新	CVE-2010-2729 打印服务 RCE CVE-2008-4250 Windows Server Service RPC RCE CVE-2012-3015 Step7 安全库加载 CVE-2010-2772 WinCC 默认口令 MS09-025 NtUserRegisterClassExWow /NtUserMessagerCall EOP	通过感染Step7项目文件 通过USB实现自启动 网络共享 Windows Server RPC Printer spooler WinCC服务器 通过RPC更新对等网络	主要基于Tilded平台	针对S7-300（315）PLCs的代码（控制了旋转离心机的速度） 针对417 PLCs的不完整的代码序列
1.100	2010/3/1 2010/4/14	二进制编译时间戳更新	CVE-2010-3888 任务调度程序EOP CVE-2010-2743 LoadKeyboardLayout EOP CVE-2010-2729 打印服务 RCE CVE-2008-4250 Windows Server Service RPC RCE CVE-2012-3015 Step7 安全库加载 CVE-2010-2772 WinCC 默认口令 CVE-2010-2568 Shortcut .lnk RCE	Step7项目文件 通过USB触发CVE-2010-2568 网络共享 Windows Server RPC Printer spooler WinCC服务器 通过RPC更新对等网络		

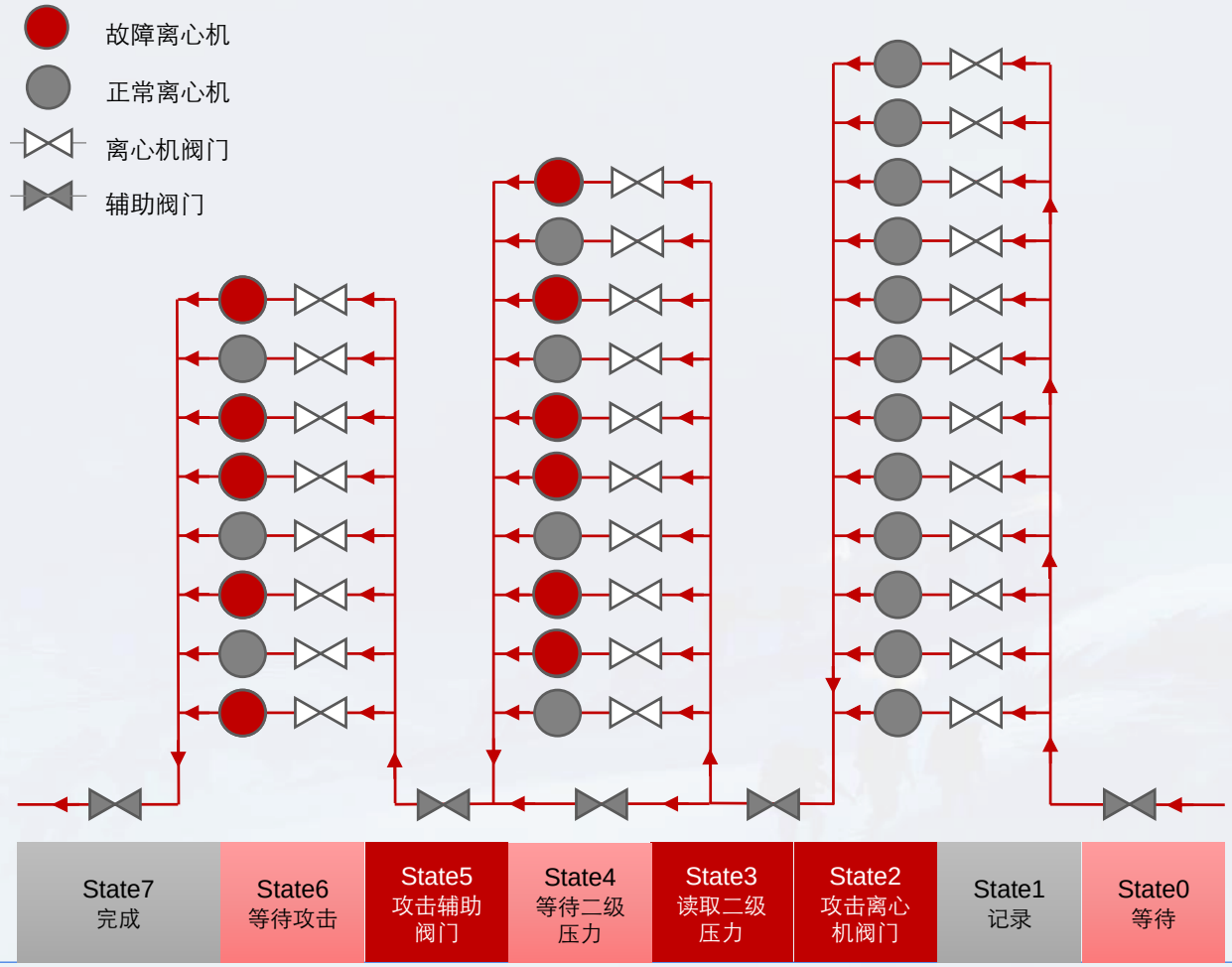
0.5和1.X版本的攻击手段差异

IR-1型离心机

0.5版本：S7-400（417）通过控制阀门改变压力，导致离心机的损坏。

1.X版本：S7-300（315）通过改变离心机的转速实现离心机的损坏。

此内容引自Symantec Stuxnet的相关分析资料



初始入侵方式

- **人力作业**
  - 据雅虎新闻采访的人士透露，荷兰特工作业，初始感染工业网络，网空威胁对抗实质上已经与人员、传统电磁信号、网络数据结合，密不可分。
- **供应链入侵**

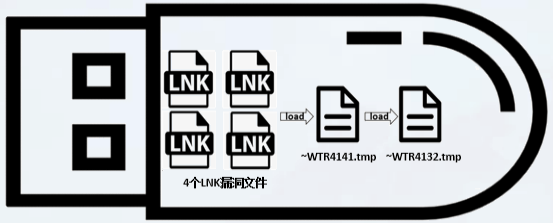
公司	地理位置	被攻击时间	主要业务
FOOLAD Technic Engineering Co(FIECO)	伊朗伊斯法罕	2009/6/23 2010/4/26	该公司为伊朗工业设施（主要为生产钢铁和电力）生产自动化系统，拥有许多伊朗最大的工业企业的数据、图纸和计划。
Behpajooh Co. Elec & Comp. Engineering	伊朗伊斯法罕	2009/6/28 2010/3/23 2010/5/13 2010/7	开发工业自动化系统，拥有SCADA/PLC的专家。
Neda Industrial Group	伊朗	2009/7/7	为水电站、水泥、以及石油、天然气及石化领域提供工业自动化服务。
Control-Gostar Jahed Company	伊朗	2009/7/7	伊朗的一家工业自动化公司，与伊朗最大的石油生产、冶金、能源等企业有着非常深入的合作。
Kala Electric	伊朗	2010/5/11	是铀浓缩离心机设备IR-1最主要的供应商，报道称在1997年至2002年间，伊朗在Kala组装和测试IR-1。
Mobarakeh Steel Company(MSC)	伊朗	2010/4/24	该公司是伊朗最大的钢铁制造商，伊朗经营规模最大的工业园区之一。

同期受到震网攻击的伊朗基础工业厂商

U盘摆渡，不是无条件传播

感染震网的计算机会监控接入的设备，一旦发现U盘插入且满足条件即开始写入U盘摆渡文件，具体条件如下：

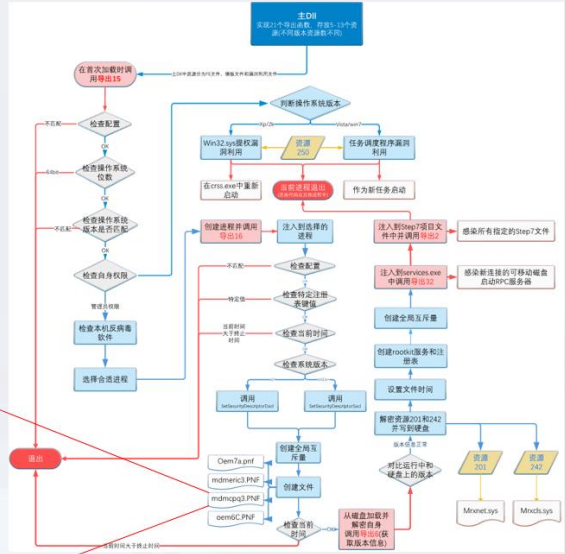
- 当前时间的U盘没有被感染；
- 根据配置标记（不是默认设置）来感染磁盘，如果默认配置不感染，那么感染的发生取决于日期；
- 感染当前计算机少于21天；
- U盘至少有5MB的剩余空间；
- U盘至少有3个文件。



偏移	长度	解释
+00	Dword	配置文件起始标志
+04	Dword	配置文件头长度
+08	Dword	配置文件校验和
+0C	Dword	配置文件长度
+68	Dword	标志位，若为 0 则检查+70 处标志（为 1 则直接感染 USB）
+70	Dword	标志位 若为 0 则检查+78 处的时间戳
+78	Qword	终止感染 USB 的时间
+80	Dword	在 USB 上需存在的文件数
+8C	Qword	终止时间
+A4	Qword	开始感染时间（超过此时间 21 天，则停止对 USB 进行感染）
…	…	…

```
0000h: 09 05 79 AE 14 00 00 00 76 FB BD 9E 44 07 00 00  ..y®....vûº½ž D...
0010h: 4C 04 00 00 03 00 00 00 01 00 00 00 02 00 00 00  L...............
0020h: 08 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00  ................
0030h: E0 93 04 00 E0 70 72 00 80 84 1E 00 FE 04 00 00  à"..àpr.€„..þ...
0040h: 01 00 00 00 01 00 00 00 01 00 00 00 80 EE 36 00  ............€î6.
0050h: 64 00 00 00 2C 01 00 00 58 02 00 00 84 03 00 00  d...,...X.....„..
0060h: 50 46 00 00 08 52 00 00 01 00 00 00 00 00 00 00  PF...R..........
0070h: 00 00 00 00 15 00 00 00 00 00 CB AA 7D A8 CB 01  ..........Ë*}¨Ë.
0080h: 03 00 00 00 40 4B 4C 00 03 00 00 00 00 C0 45 4C  ....@KL......ÀEL
0090h: 9C 51 CD 01 38 31 00 00 00 00 00 00 00 00 00 00  œQÍ.81..........
00A0h: 00 00 00 00 10 02 B2 7B CC 40 CA 01 01 00 00 00  ......²{Ì@Ê.....
00B0h: 00 00 00 00 10 02 B2 7B CC 40 CA 01 00 00 00 00  ......²{Ì@Ê.....
00C0h: 5A 00 00 00 87 00 00 00 01 00 00 00 77 00 77 00  Z...‡.......w.w.
00D0h: 77 00 2E 00 77 00 69 00 6E 00 64 00 6F 00 77 00  w...w.i.n.d.o.w.
00E0h: 73 00 75 00 70 00 64 00 61 00 74 00 65 00 2E 00  s.u.p.d.a.t.e...
00F0h: 63 00 6F 00 6D 00 00 00 00 00 00 00 00 00 00 00  c.o.m...........
```

……



事后大面积感染的三种猜测

作业方失误

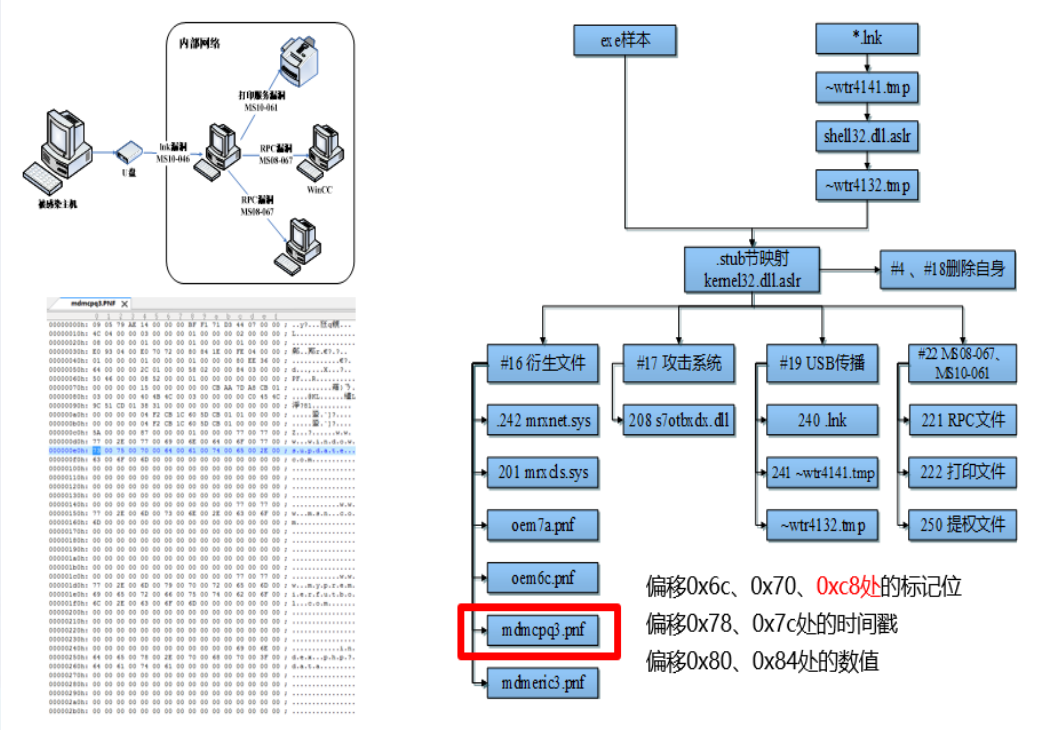
- 由于传播条件控制错误，导致在互联网传播；可能在工程商服务商接入工业内网维护时感染他们的笔记本，进而又工程商服务商的笔记本传播到其他客户内网；如此循环，导致不断在各种基础设施内网中传播，这其中有的网络存在VPN，最终导致震网的传播失控。

作业方蓄意/干扰和混淆

- 以达成作业意图后大规模感染，掩盖定向攻击行为和意图，干扰溯源分析。

作业方蓄意/能力展示

- 这是美国军事历史上又一释放卫星的时刻，因为不可能到阅兵式上去展示U盘——《震网蠕虫的秘密变种》。

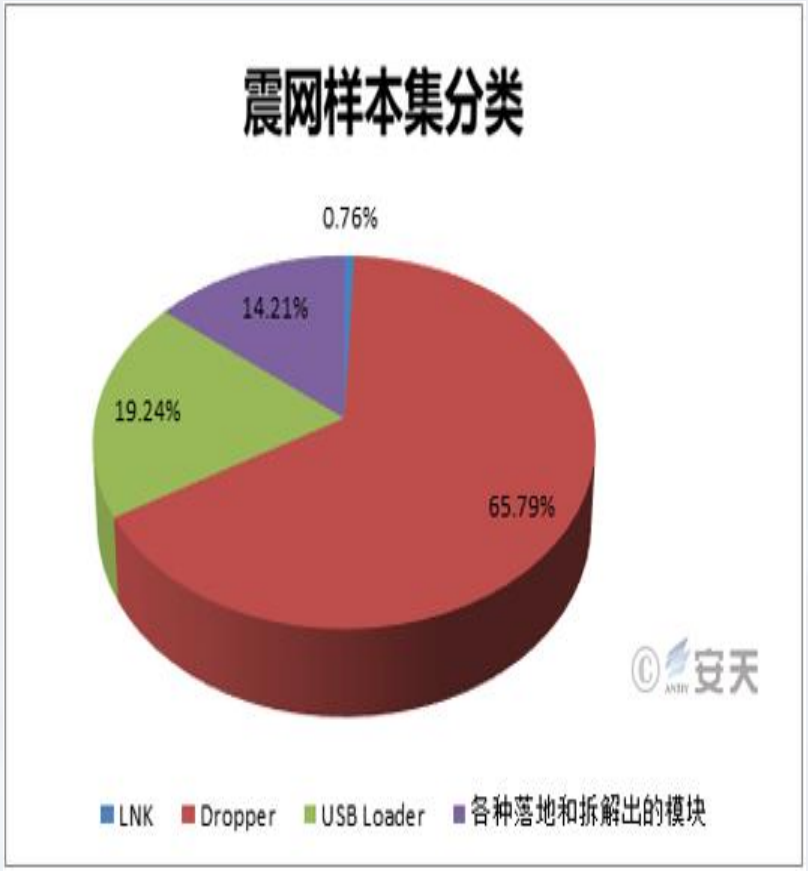


USB传播开关默认是关闭的

来源：安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》，2012年9月首发

震网为何有数千个样本

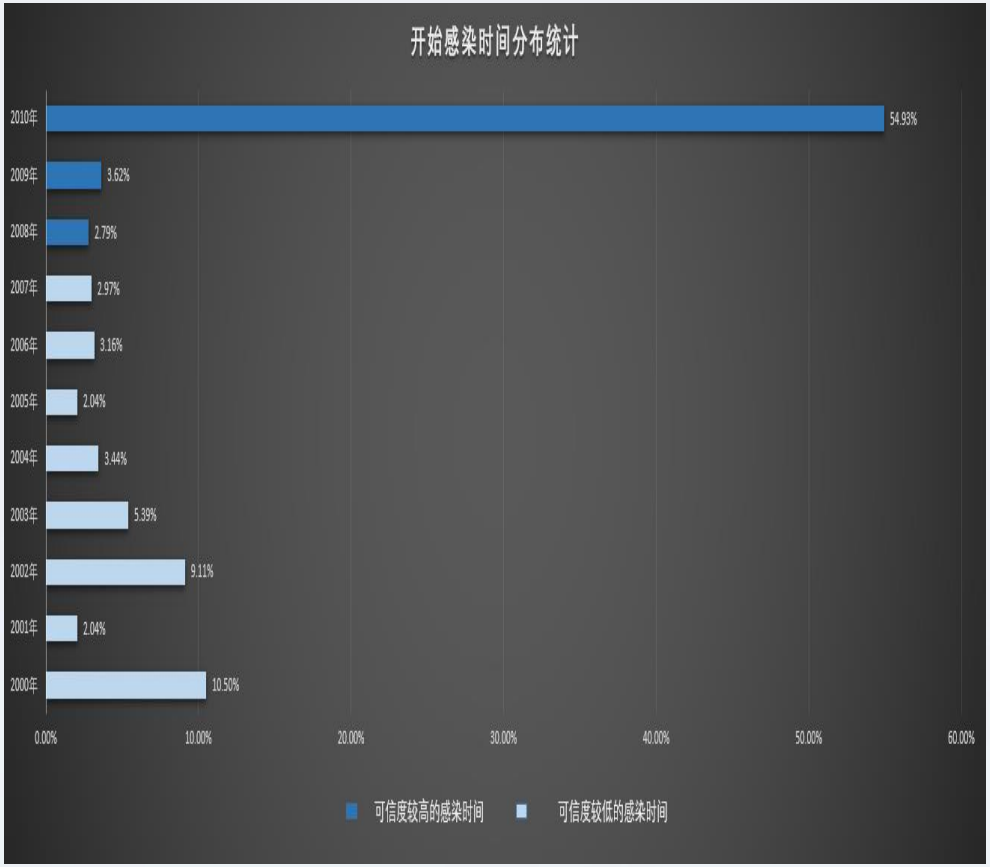
- **1. Dropper样本在落地时写入目标配置导致文件变化**
  - stub段中存储的配置数据会被当前感染节点的相关信息数据更新，这是导致震网样本集数量多的一个最主要原因。也就是说，每次落地震网都会再形成一个HASH不同的Dropper。
- **2. 分析提取工作导致**
  - 因Dump导致的不同版本，未脱壳版本，不同脱壳方式生成的文件有差异.
- **3. 干扰数据**
  - 在震网的USB Loader样本集中，有数以百计的样本文件签名损坏，且大量该类文件的尾部还追加了其他的LNK文件和某种反病毒产品的报警日志，从目前分析来看，可能是某安全产品的产品BUG导致的，其某版本在扫描样本时，会错误的样本后面追加数据，从而引入数百被破坏的样本。

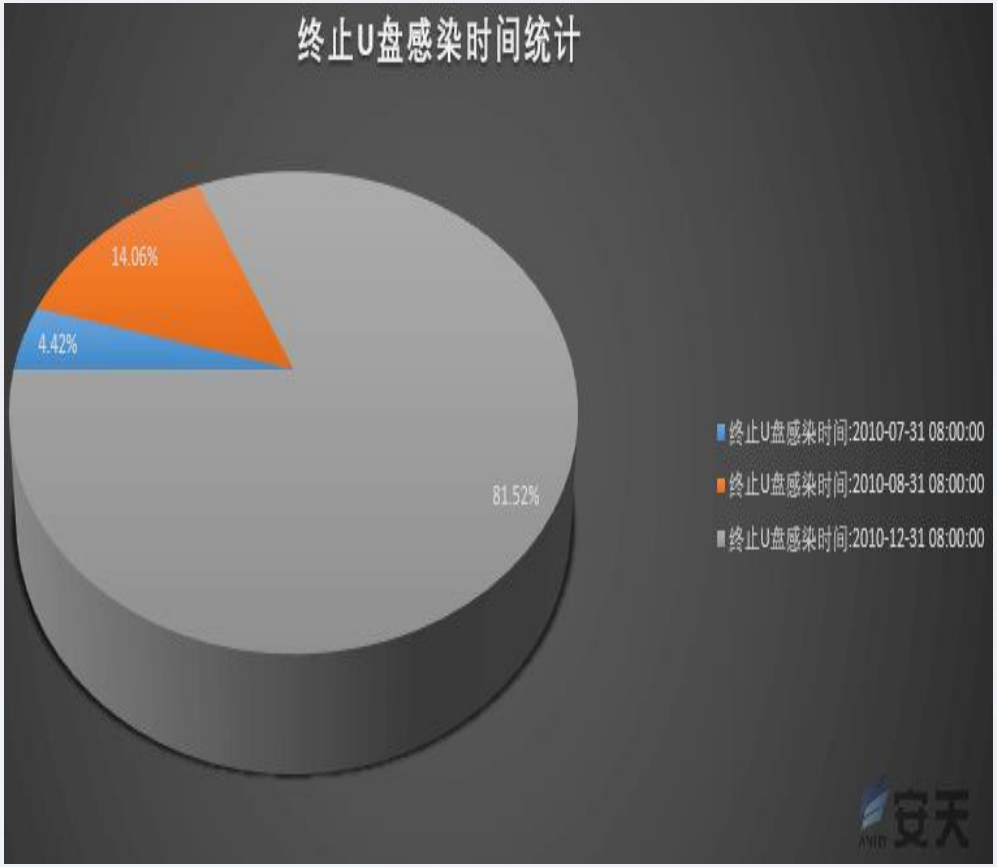


解密后的部分感染计算机信息

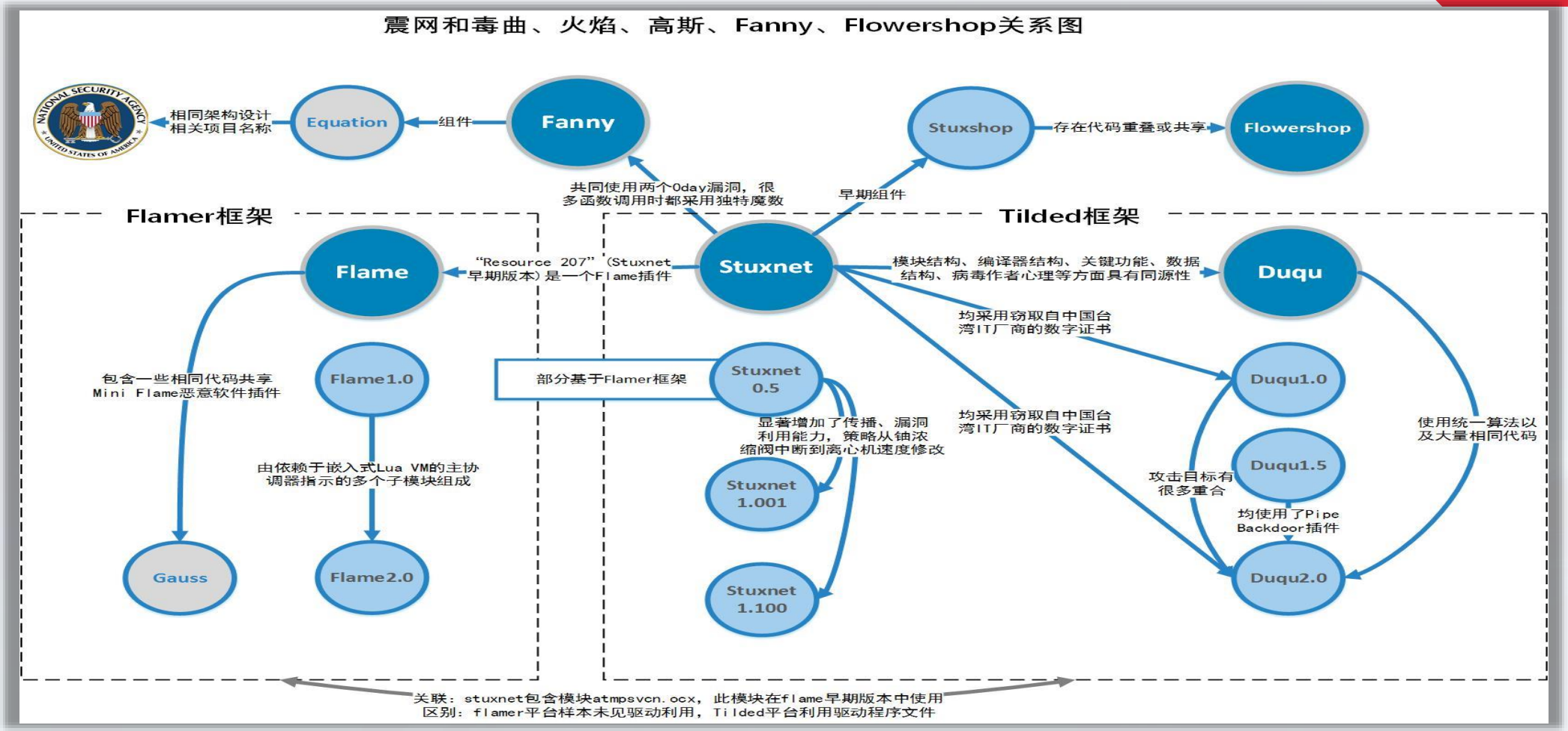
计算机名	域名	感染时间	系统版本	ip1	ip2	ip3
computer:YOUNG	domain:SYNTEC	infect time:1802/01/03 00:35	version:0500	ip1:0.0.0.0.	ip2:192.168.0.7.	ip3:0.0.0.0.
computer:YOUR-8C02652B41	domain:WORKGROUP	infect time:1980/01/03 22:24	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:MONJU	domain:RTIP	infect time:1980/01/04 02:05	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:SYED-S	domain:WORKGROUP	infect time:1980/01/04 02:32	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:ENG	domain:DTEGEN	infect time:1980/01/04 02:39	version:0501	ip1:192.168.100.138.0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:HOME-D1F751021B	domain:WORKGROUP	infect time:1980/01/04 02:50	version:0501	ip1:10.205.200.89.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:QURBAN-7A0EF802	domain:WORKGROUP	infect time:1980/01/04 03:32	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:QURBAN-0914A4CF	domain:WORKGROUP	infect time:1980/01/04 03:32	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:QURBAN-F75188C1	domain:WORKGROUP	infect time:1980/01/04 03:33	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:QURBAN-4B880F25	domain:WORKGROUP	infect time:1980/01/04 03:48	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:MLTNET	domain:PSMCHS	infect time:1980/01/04 05:05	version:0501	ip1:192.168.80.60.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:HPD530	domain:PSMCHS	infect time:1980/01/04 05:08	version:0501	ip1:192.168.80.60.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:USER-4B9213D38F	domain:WORKGROUP	infect time:1980/01/04 05:26	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:6609E26B57334EA	domain:WORKGROUP	infect time:1980/01/04 06:25	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:COMPAQ-29F0F7E2	domain:WORKGROUP	infect time:1980/01/04 07:36	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:USER	domain:WORKGROUP	infect time:1980/01/04 07:54	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:DINGAM	domain:COTONTCHAD	infect time:1980/01/04 10:31	version:0501	ip1:0.0.0.0.	ip2:192.168.10.150.	ip3:0.0.0.0.
computer:SYS1	domain:WORKGROUP	infect time:1980/01/04 10:45	version:0501	ip1:169.254.136.200.0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:YOUR-E04A529035	domain:WORKGROUP	infect time:1980/01/04 16:00	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:Q-0E5444BB6EB84	domain:WORKGROUP	infect time:1980/01/04 16:01	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:SPUR-3472F2F832	domain:WORKGROUP	infect time:1980/01/04 16:03	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:05599292-879DE1	domain:WORKGROUP	infect time:1980/01/04 16:25	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:PRIVATE-CD91EAC	domain:WORKGROUP	infect time:1980/01/04 17:21	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:THORAYA	domain:MSHOME	infect time:1980/01/04 18:08	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:WWW-704916C5815	domain:WORKGROUP	infect time:1980/01/04 19:12	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:ABC	domain:WORKGROUP	infect time:1980/01/13 08:35	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:AAM	domain:WORKGROUP	infect time:1980/02/19 08:17	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:TEACHER	domain:MSHOME	infect time:1981/10/19 06:08	version:0501	ip1:0.0.0.0.	ip2:192.168.1.254.	ip3:0.0.0.0.
computer:CRYSTAL_XP	domain:WORKGROUP	infect time:1988/01/01 01:04	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:USER-A10E71981B	domain:WORKGROUP	infect time:1988/01/01 01:04	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:AMBUSADE-CF25D0	domain:WORKGROUP	infect time:1988/01/01 03:50	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:VISTA	domain:MSHOME	infect time:1988/01/01 05:04	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:CGD-FF4C30E0004	domain:WORKGROUP	infect time:1988/01/01 16:02	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:USER-106BEB0698	domain:WORKGROUP	infect time:1988/01/01 16:25	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:RAGNA	domain:WORKGROUP	infect time:1990/01/01 01:08	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:ANAND1	domain:PRISM	infect time:1990/01/01 03:33	version:0501	ip1:192.168.0.123.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:23A194CF75E94B4	domain:WORKGROUP	infect time:1990/01/01 06:01	version:0500	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:NAREN-88DBADC92	domain:WORKGROUP	infect time:1995/06/29 21:47	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:M4MLUX-M4F14	domain:WORKGROUP	infect time:1996/03/15 09:25	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:COMP-1900000806	domain:WORKGROUP	infect time:1997/01/01 05:01	version:0500	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:GFHHH	domain:WORKGROUP	infect time:1997/01/19 13:28	version:0501	ip1:0.0.0.0.	ip2:0.0.0.0.	ip3:0.0.0.0.
computer:PC10	domain:MSHOME	infect time:1997/02/01 12:34	version:0501	ip1:192.168.1.110.	ip2:0.0.0.0.	ip3:0.0.0.0.

开始感染时间与终止感染时间





大规模恶意代码的工程体系与事件关联

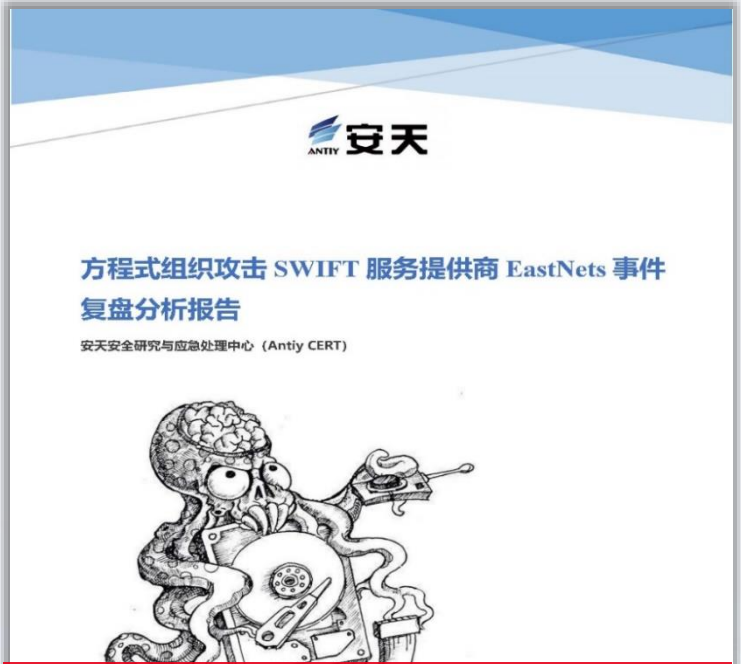


寒夜遠征

威胁框架：认知与实践

02 中东SWIFT服务商被入侵复盘

复盘超级网空威胁行为体的一次完整攻击行动



2019年6月1日

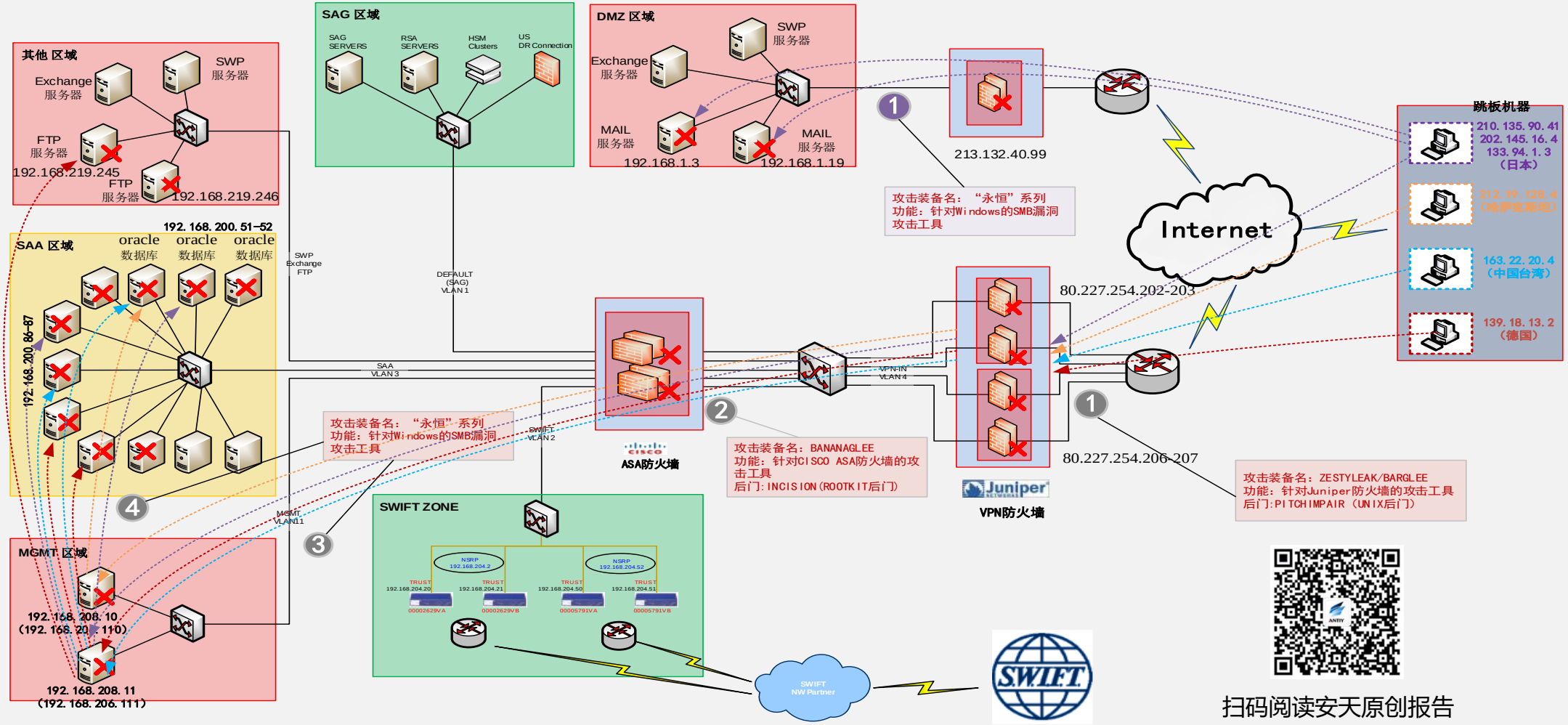
安天基于多年持续跟踪分析超高能力网空威胁行为体的分析成果，以态势感知视角，完整复盘方程式组织攻击中东最大SWIFT服务商的完整过程，并从威胁框架层面进行映射解读。

扫码阅读安天原创报告

2019年6月13日

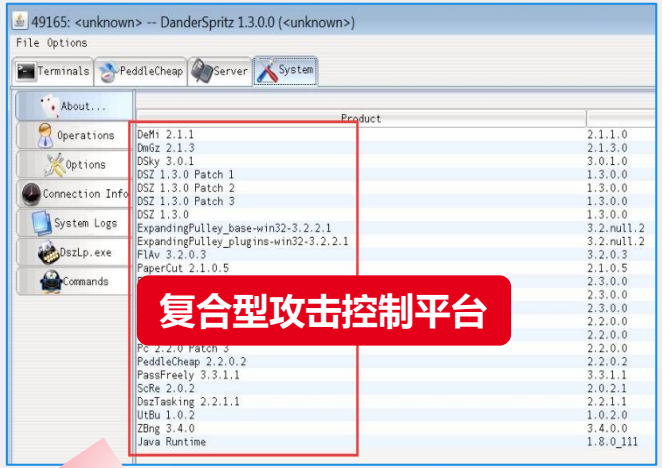
新华社发文批判美方滥用网络攻击能力，危害网络空间秩序的行为。其中援引了安天发布的《方程式组织攻击中东SWIFT服务商事件复盘分析报告》的相关分析作为佐证。

“方程式组织”入侵EastNets行动中受到入侵和影响的资产

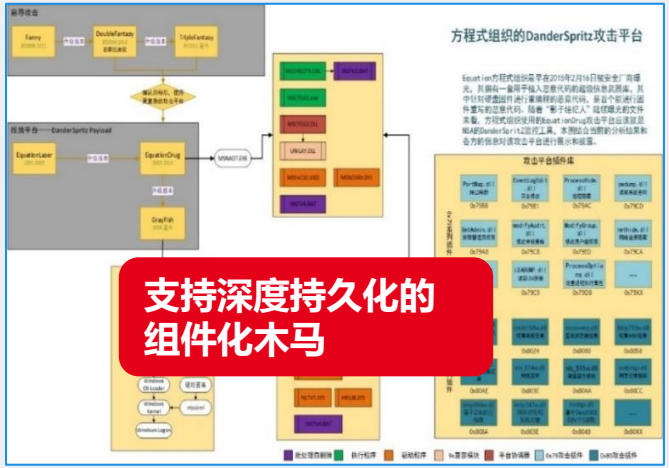


从入侵SWIFT看装备体系和推进过程

针对各种主流IT场景运载、植入和持久化、和传输中继工具

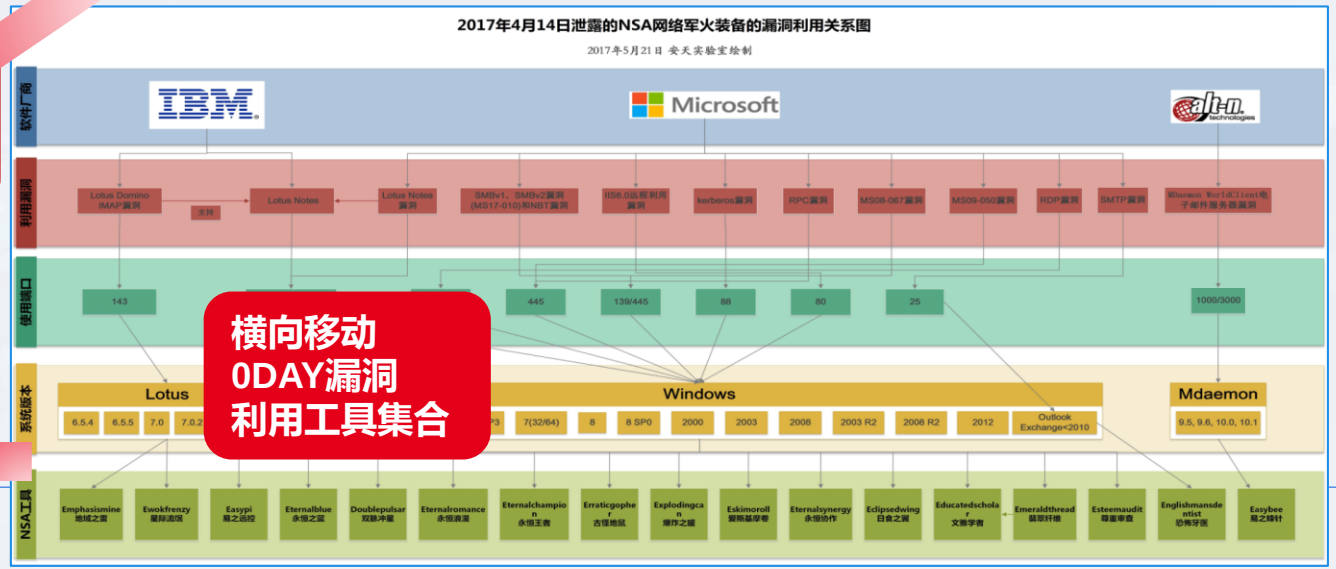


复合型攻击控制平台



支持深度持久化的组件化木马

装备名称	针对产品
ZESTYLEAK	针对Juniper防火墙的攻击工具
BARGLEE	针对Juniper防火墙的攻击工具
BANANAGLEE	一个用于植入CISCO ASA和PIX系列设备的非持续控制工具集合（只驻留于内[illegible]启后失效），目的是在获取防火墙权限后，能够实现对设备的控制。
PITCHIMPAIR	Unix后门工具
INCISION	具有Rootkit功能的后门工具
FuzzBunch	FB平台是漏洞利用工具，可植入后门。
DanderSpritz	DS平台是远程控制程序的客户端，可在被植入后门的机器上执行各种操作。
ETERNALROMANCE	永恒系列攻击工具，ETERNALROMANCE (永恒浪漫) 是影响Windows全平台的SMBv1远程代码执行漏洞攻击工具，受影响的系统为Windows XP, Vista, 7, Windows Server 2003/2008/ 2008 R2等
ETERNALCHAMPION	永恒系列攻击工具，ETERNALCHAMPION（永恒冠军）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows Server 2008 SP1 x86等
ETERNALSYNERGY	永恒系列攻击工具，ETERNALSYNERGY（永恒协作）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows 8等
ETERNALBLUE	永恒系列攻击工具，ETERNALSYNERGY（永恒之蓝）是影响Windows的SMBv1远程代码执行漏洞攻击工具.受影响的系统为Windows 7/8/XP等
EXPLODINGCAN	EXPLODINGCAN（爆炸之罐）是IIS6.0 webDAV漏洞的攻击工具。



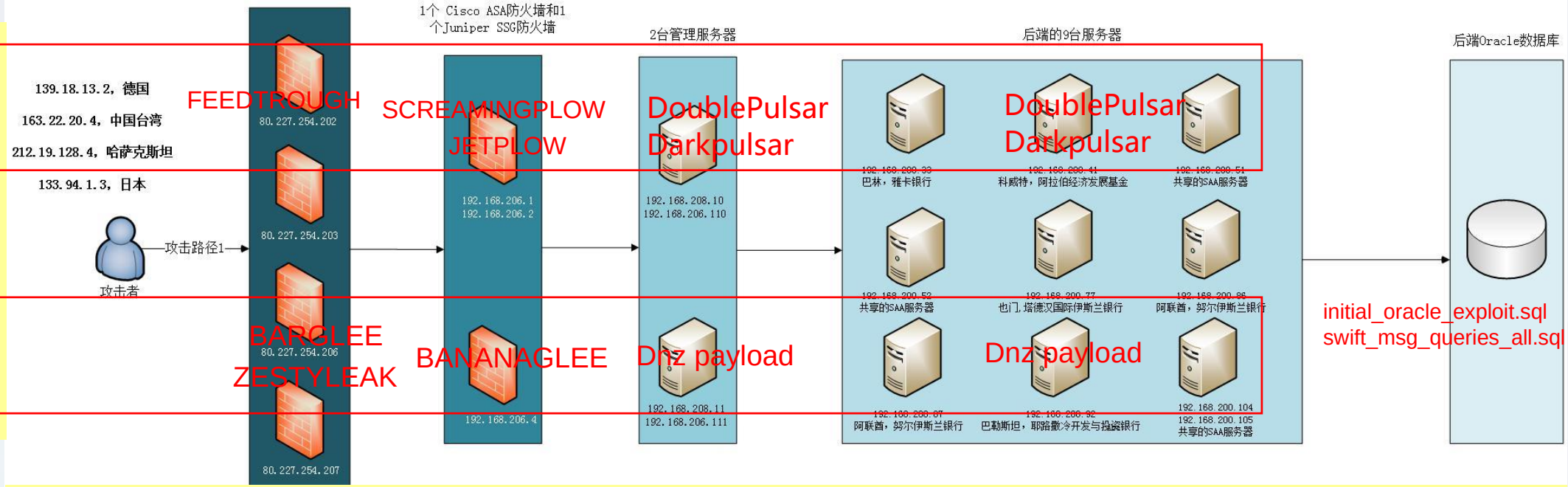
横向移动
0DAY漏洞
利用工具集合

攻击流程及武器工具分布图

突破/漏洞利用武器：
EBBISLAND　CVE-2015-7755　EPICBANANA　FB平台Eternal系列漏洞　PASSFREELY

植入武器

植入物



全程使用流量转发/重定向武器：　NOPEN　INCISION　PITCHIMPAIR

攻击工具：漏洞利用武器

工具名称	功能和针对目标
EBBISLAND / EBBSHAVE（CVE-2017-3623）	针对UNIX系统主机的漏洞攻击武器，针对SOLARIS6-10的漏洞利用武器，未经身份验证的远程攻击者可以通过特制的RPC请求利用此漏洞来执行任意代码。
名称未知（CVE-2015-7755）	Juniper ScreenOS 中的一个身份认证绕过漏洞，通过 SSH 或 TELNET 登录 ScreenOS 设备，只需要登录授权认证中包中密码指定为后门密码 <<< %s(un='%s') = %u 皆可绕过 ScreenOS 身份认证，获取设备管理员权限。
EPICBANANA（CVE-2016-6367）	针对Cisco ASA and PIX设备的漏洞攻击武器，允许经过身份验证的攻击者创建拒绝服务（DoS）或执行任意代码。攻击者可以通过在受影响的设备中调用某些无效命令来利用此漏洞。攻击者必须知道telnet或SSH密码才能成功利用受影响的设备。
EXTRABACON（CVE-2016-6366）	针对Cisco ASA 设备的SNMP漏洞攻击武器，允许经过身份验证的远程重启系统或远程执行代码。
Eternal系列漏洞攻击工具（CVE-2017-0143）	针对Windows、IIS、Lotus的漏洞攻击武器，SMB、RDP漏洞，攻击成功后可以远程执行代码。
PassFreely	Oracle (7.2 -> 11.2)数据库登录验证绕过武器。

植入武器与植入物

工具名称	功能介绍
NOPEN	针对UNIX系统的后门武器，可确定具有流量重定向功能
PITCHIMPAIR	Unix后门工具可能具有重定向流量功能
INCISION	具有Rootkit功能的后门工具可能具有重定向流量功能
JETPLOW	针对 Cisco ASA and PIX设备进行植入的武器
SCREAMINGPLOW	
BANANAGLEE	针对Cisco ASA and PIX设备的内存非持久化植入物，非持续控制工具集合（只驻留于内存中，重启后失效），目的是在获取防火墙权限后，能够实现对设备的控制。
BANANABALLOT	针对设备的BIOS的植入物（与BANANAGLEE类似）
BEECHPONY	针对Cisco ASA and PIX设备的内存非持久化植入物，BANANAGLEE的前身
FEEDTROUGH	针对Juniper NetScreen firewalls设备进行植入的武器
BARGLEE	Juniper NetScreen firewalls的植入物
ZESTYLEAK	
DoublePulsar	针对WindowS系统的内核级植入的武器
Darkpulsar	
Dnz平台Payload	针对Windows系统的内存进程植入物

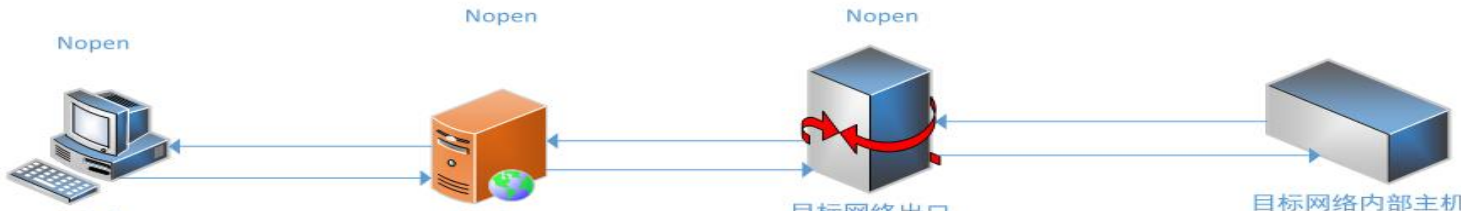
Windows文件夹——NSA/DS-FB攻击平台结构简析

NSA/DS-FB攻击平台结构简析

DanderSpritz/支持命令					fuzzbunch		
平台管理	进程操作	文件操作	kisu模块存储库	网络操作	内置漏洞（exploits文件夹）	漏洞扫描工具集（touches文件夹）	后渗透阶段载荷及插件（payloads文件夹）
commands	cprpc	checksum	kisu_fulllist	domaincontroller	Easybee 1.0.1 Mdaemon漏洞	Architouch	Doublepulsar
addresses	debug	database	kisu_addmodule	banner	Easypi 3.1.0 IBM Lotus漏洞	Domaintouch	Jobadd
aliases	handles	copy	kisu_config	arp	Eclipsedwing 1.5.2 MS08－067	Eclipsedwingtouch	Jobdelete
activedirectory	hide	copyget	kisu_connect	keepalive	Educatedscholar 1.0.0 MS09－050	Educatedscholartouch	Joblist
available	debugload	delete	kisu_loadmodule	nsg	Emeraldthread 3.0.0 MS10－061	Emeraldthreadtouch	Pcdlllauncher
cd	injectdll	gangsterthief	kisu_processload	packetredirect	Emphasismine 3.4.0 IBM Lotus Domino漏洞	Erraticgophertouch	Processlist
freeplugin	processconnections	mkdir	kisu_readmodule	nameserverlookup	Englishmansdentist 1.2.0 OUTLOOK EXCHANGE漏洞	Esteemaudittouch	Regdelete
frzlinks	processes	move	kisu_survey	netmap	Erraticgopher 1.0.1 SMB漏洞	Explodingcantouch	Regenum
frzroutes	processinfo	strings	kisu_uninstall	knock	Eskimoroll 1.1.1 MS14－068	Iistouch	Regread
frzaddress	processmemory	systempaths	kisu_upgrade	ping	Esteemaudit 2.1.0 RDP漏洞	Namedpipetouch	Regwrite
break	processmodify	rmdir	kisu_usebh	portmap	Eternalromance 1.4.0 SMBv1 漏洞	Printjobdelete	Rpcproxy
help	processoptions	logedit	kisu_install	randdirect	Eternalsynergy 1.0.1 SMB漏洞	Printjoblist	Smbdelete
hour	processsuspend	filetype	kisu_list	route	Ewokfrenzy 2.0.0 Domino漏洞	Rpctouch	Smblist
渗透相关	远控生成连接指令	dsky脚本指令	注册表操作	硬件操作	向目标机器植入指定程序（implants文件夹）	影响较大的漏洞（specials文件夹）	
activity	pc2.2_uninstall	dsky_deletecapture	appcompat	drivers	Darkpulsar	Eternalblue/永恒之蓝	
darkskyline	pc2.2_upgrade	dsky_getcapture					
duplicatetoken	pc_connect	dsky_getfilter	performance	devicequery			
authentication	pc_install	dsky_install					
acquiretoken	pc_listen	dsky_load	registryadd	dmgz_control			
eventlogfilter	pc_master	dsky_setmaxsize					
eventlogquery	pc_pick	dsky_start	registryquery	flav_control			
eventlogsearch	pc_pick	dsky_status					
firewall	pc_status	dsky_stop	registrydelete	flav_plugins	Mofconfig	Eternalchampion	
forcelogon	pc_uninstall	dsky_uninstall					
eventlogclear	pc_upgrade	dsky_unload	appcompat_uninstal l	diskspace			
getadmin	pc2.2_install	dsky_verifyinstall					
logonasuser	pc2.2_pick	dsky_verifyrunning	registryhive	drives			
.....							

内网流量重定向渗透攻击武器NOPEN

Nopen复盘：



实验数据：

攻击者
ip:192.168.37.131
监听端口：6789
转发：192.168.37.130：4567

跳板机
ip:192.168.37.130
监听端口：4567
转发：192.168.37.129：8888

目标网络出口
ip:192.168.37.129
监听端口：8888
转发：192.168.37.1：8888

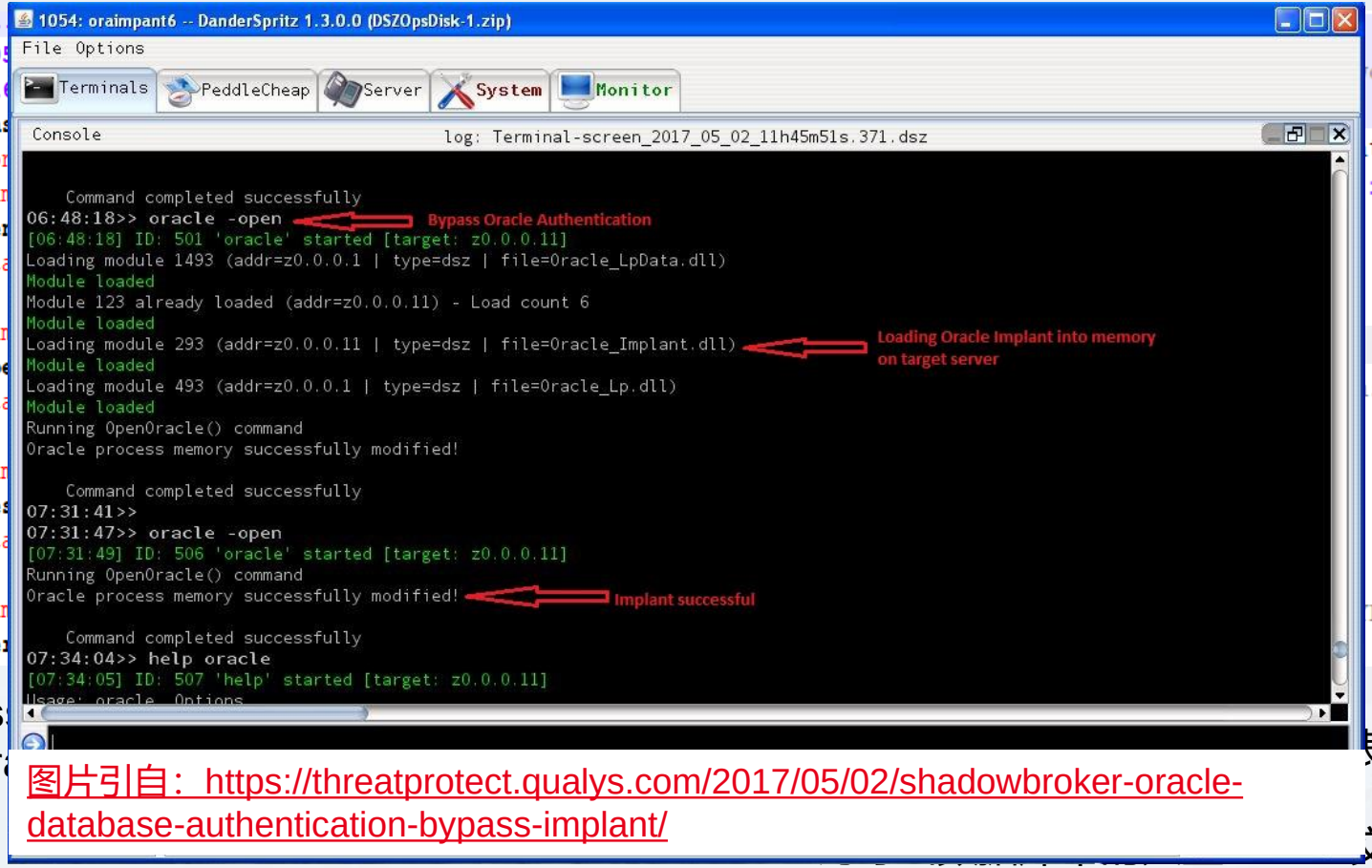
目标网络内部主机
ip:192.168.37.1
服务：8888端口存在网站

实验抓取流量包

69	13:04:41.035248	192.168.37.129	192.168.37.1	TCP	60	34209 → 8888 [ACK] Seq=1 Ack=1 Win=29200 Len=0
70	13:04:43.598616	192.168.37.131	192.168.37.130	HTTP	444	GET HTTP/1.1
71	13:04:43.598794	192.168.37.130	192.168.37.131	TCP	66	4567 → 42047 [ACK] Seq=1 Ack=379 Win=64782 Len=0 TSval=3565640 TSecr=2960445421
72	13:04:43.603559	192.168.37.130	192.168.37.129	HTTP	444	GET HTTP/1.1
73	13:04:43.603834	192.168.37.129	192.168.37.130	TCP	66	8888 → 39649 [ACK] Seq=1 Ack=379 Win=30032 Len=0 TSval=2384158868 TSecr=1595829808
74	13:04:43.604232	192.168.37.129	192.168.37.1	HTTP	432	GET HTTP/1.1
75	13:04:43.645398	192.168.37.1	192.168.37.129	TCP	54	8888 → 34209 [ACK] Seq=1 Ack=379 Win=1051136 Len=0
76	13:04:43.685717	192.168.37.1	192.168.37.129	TCP	71	8888 → 34209 [PSH, ACK] Seq=1 Ack=379 Win=1051136 Len=17 [TCP segment of a reassembled PDU]
77	13:04:43.685935	192.168.37.129	192.168.37.1	TCP	60	34209 → 8888 [ACK] Seq=379 Ack=18 Win=29200 Len=0
78	13:04:43.685958	192.168.37.1	192.168.37.129	HTTP	473	HTTP/1.0 200 OK (text/html)
79	13:04:43.686516	192.168.37.129	192.168.37.1	TCP	60	34209 → 8888 [FIN, ACK] Seq=379 Ack=438 Win=30272 Len=0
80	13:04:43.686539	192.168.37.1	192.168.37.129	TCP	54	8888 → 34209 [ACK] Seq=438 Ack=380 Win=1051136 Len=0
81	13:04:43.686678	192.168.37.129	192.168.37.130	HTTP	502	HTTP/1.0 200 OK (text/html)
82	13:04:43.686893	192.168.37.130	192.168.37.129	TCP	66	39649 → 8888 [ACK] Seq=379 Ack=437 Win=64088 Len=0 TSval=1595829896 TSecr=2384158951
83	13:04:43.687054	192.168.37.129	192.168.37.130	TCP	66	8888 → 39649 [FIN, ACK] Seq=437 Ack=379 Win=30032 Len=0 TSval=2384158951 TSecr=1595829896
84	13:04:43.687355	192.168.37.130	192.168.37.129	TCP	66	39649 → 8888 [FIN, ACK] Seq=379 Ack=438 Win=64088 Len=0 TSval=1595829896 TSecr=2384158951
85	13:04:43.687482	192.168.37.130	192.168.37.131	HTTP	502	HTTP/1.0 200 OK (text/html)
86	13:04:43.687636	192.168.37.130	192.168.37.131	TCP	66	4567 → 42047 [FIN, ACK] Seq=437 Ack=379 Win=64782 Len=0 TSval=3565729 TSecr=2960445421
87	13:04:43.687702	192.168.37.131	192.168.37.130	TCP	66	42047 → 4567 [ACK] Seq=379 Ack=437 Win=64088 Len=0 TSval=2960445510 TSecr=3565729
88	13:04:43.688131	192.168.37.131	192.168.37.130	TCP	66	42047 → 4567 [FIN, ACK] Seq=379 Ack=438 Win=64088 Len=0 TSval=2960445511 TSecr=3565729
89	13:04:43.688608	192.168.37.130	192.168.37.131	TCP	66	4567 → 42047 [ACK] Seq=438 Ack=380 Win=64782 Len=0 TSval=3565730 TSecr=2960445511

实际攻击流程：

Oracle (7.2 -> 11.2)登录验证的攻击武器



图片引自：https://threatprotect.qualys.com/2017/05/02/shadowbroker-oracle-database-authentication-bypass-implant/

DS平台Pas

攻击绕过Ora

表以及访问凭据

交易记录

网空威胁框架分析“SWIFT”

Administration（行动管理与资源保障）			Preparation（目标勘察与环境整备）		Engagement（接触目标与进攻突防）		Presence（持久化驻留潜伏）						Effect（致效能力运用）					Ongoing Processes（全程持续支撑作业）			
规划	资源开发	研究	侦察	环境预置	投递	利用	执行	内部侦察	提权	凭证访问	横向移动	持久化	监控	渗出	修改	拒绝	破坏	分析、评估、反馈	命令与控制	规避	
分析行动	获取行动所需基础设施	收集信息	执行社会工程学	应用数据文件中添加可利用点	无线接入	滥用协议	创建计划任务	枚举账户和权限	利用应用程序漏洞	添加或修改凭证	利用对等网络	创建新服务	激活记录	收集串扰	修改数据	破坏文件或应用程序	磁盘/操作系统变砖（全部删除）	使用基础设施	向中点发送信标	直接访问磁盘	删除日志数据
确定战略和目标	建立联盟和伙伴关系	确定能力差距	收集凭证	分配行动所需基础设施	改变通信路径	访问虚拟内存	通过服务控制器执行	枚举文件系统	利用固件漏洞	执行社会工程学	远程登录	创建计划任务	被动收集	从本地系统收集	修改进程结果	降低性能	损坏磁盘/操作系统（部分删除）	实施效果评估	建立对等网络	规避数据大小限制	删除toolkit
发布行动指令	创建僵尸网络	确定信息差距	识别串扰	建立跳板	供应链/受信源入侵	执行社会工程学	通过第三方软件执行	枚举本地网络连接	利用操作系统漏洞	破解密码	利用密码哈希认证	编辑boot记录	为其他行动创造条件	从网络资源收集	造成物理影响	中断/拒绝服务	删除数据	优化潜在受害者	中继通信	阻止主机信标上传	为恶意内容签名
制定行动计划	能力开发		测绘可访问网络	建立物理抵近点	可移动介质连接	破解加密	注入进程	枚举本地网络设置	注入进程	转储凭证	利用ticket认证	修改文件类型关联	键盘记录	压缩数据	修改机器间通信	加密数据使其不可用	破坏硬件		发送命令	降级安全产品	将文件存储在非常规的位置
获准执行行动	获得资金		扫描设备	网站植入或预埋	异常网络设备连接	利用固件漏洞	利用授权用户	枚举操作系统和软件	利用辅助功能	劫持活动的凭证	通过可移动介质复制	使用登录脚本	保持访问	泄露数据或信息	更改系统进程的运行状态				利用僵尸网络	延迟活动	根据环境调整行为
选择目标受害者	供应链 预置		爬取网站	预置载荷	通过网站感染	利用本地应用程序漏洞	替换现有二进制文件	枚举进程	利用合法凭证	定位凭证	污染共享内容	利用路径顺序执行	屏幕截屏	将数据存储到指定位置	篡改网站				利用链式协议	采用反取证措施	利用签名内容
	人员和培训资源		选择潜在受害者		注入数据库命令	利用操作系统漏洞	运行shell命令	枚举窗口		键盘记录	利用应用程序部署软件	修改BIOS		运行收集脚本	破解加密				利用对等连接	采用反逆向工程措施	
			调查设备		利用设备交换	利用远程应用程序漏洞	运行无文件载荷	测绘可访问网络			利用远程服务	修改配置用于启动		通过C2信道发送					利用远程shell	使用rootkit	
			利用社交媒体		发送恶意邮件	利用弱访问控制	利用解释脚本	扫描连接的设备			写入远程文件共享	修改现有服务		通过非C2信道发送					利用可移动介质	编码数据	
					借助公共网络基础设施传输	劫持	利用系统接口	嗅探网络			写入共享webroot目录	修改链接		通过其他网络介质发送						加密数据	
					利用CDS或MLS传输	冒充/欺骗用户	利用远程服务					修改服务配置		节流数据						仿冒合法文件	
					利用聊天服务	零日漏洞利用	通过受信应用执行非受信应用					替换服务二进制文件		通过物理方法传输						操纵受信进程	
					利用受感染主机	漏洞利用工具包	写入磁盘					设置为启动时加载		利用CDS或MLS传输						仿冒合法流量	
					利用合法远程访问	利用受信关系						利用库搜索劫持								修改恶意代码以规避检测	
					利用物理网桥	重放攻击														混淆数据	

确定使用的攻击手段

推测使用的攻击手段

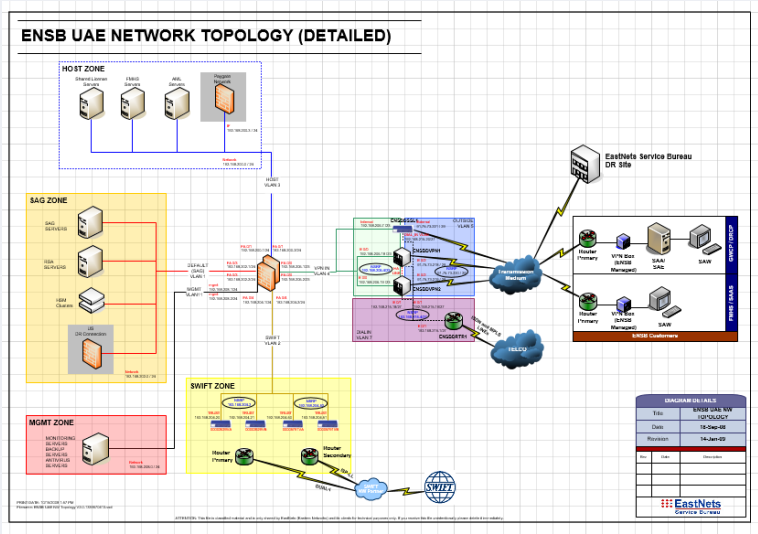
JEEPFLEA_MARKET和JEEPFLEA_POWDER

SWIFT文件夹中的内容提及到了两个攻击事件：

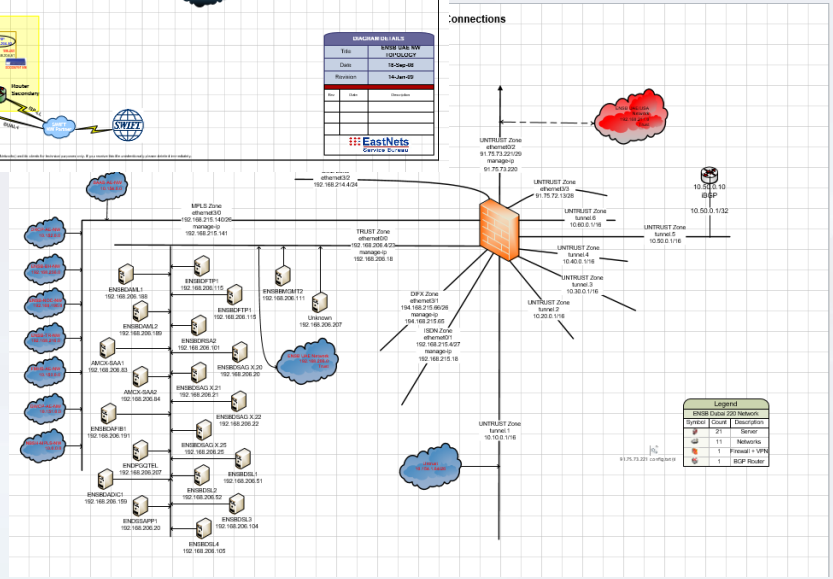
- JEEPFLEA_MARKET
  - 针对EastNets的攻击，包含了网络架构、系统密码以及几千个雇员的账号。
- ~~JEEPFLEA_POWDER。~~
  - ~~是针对EastNets合作伙伴的攻击，这个合作伙伴名为BCG（Business Computer Group），位于委内瑞拉和巴拿马。（备注：此攻击的状态为无进展）。~~

准备阶段和进入阶段的网络拓扑图

前期入侵获取——jpdm.eastnets.com-->

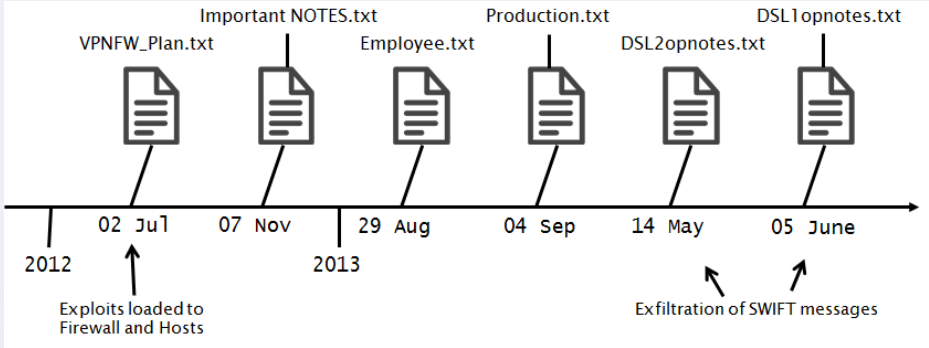


攻击者渗透绘制-->



6次入侵攻击日志、记录文件

- SWIFT文件夹中有6个文件大致描述了攻击发生的时间线
  - 《Production.txt》，139.18.13.2，德国
  - 《DSL1opnotes.txt》，163.22.20.4，中国台湾
  - 《VPNFW_Plan.txt》，212.19.128.4，哈萨克斯坦
  - 《DSL2opnotes.txt》，133.94.1.3，日本
  - 《Important NOTES.txt》，202.145.16.4，日本
  - 《Employee》，210.135.90.41，日本



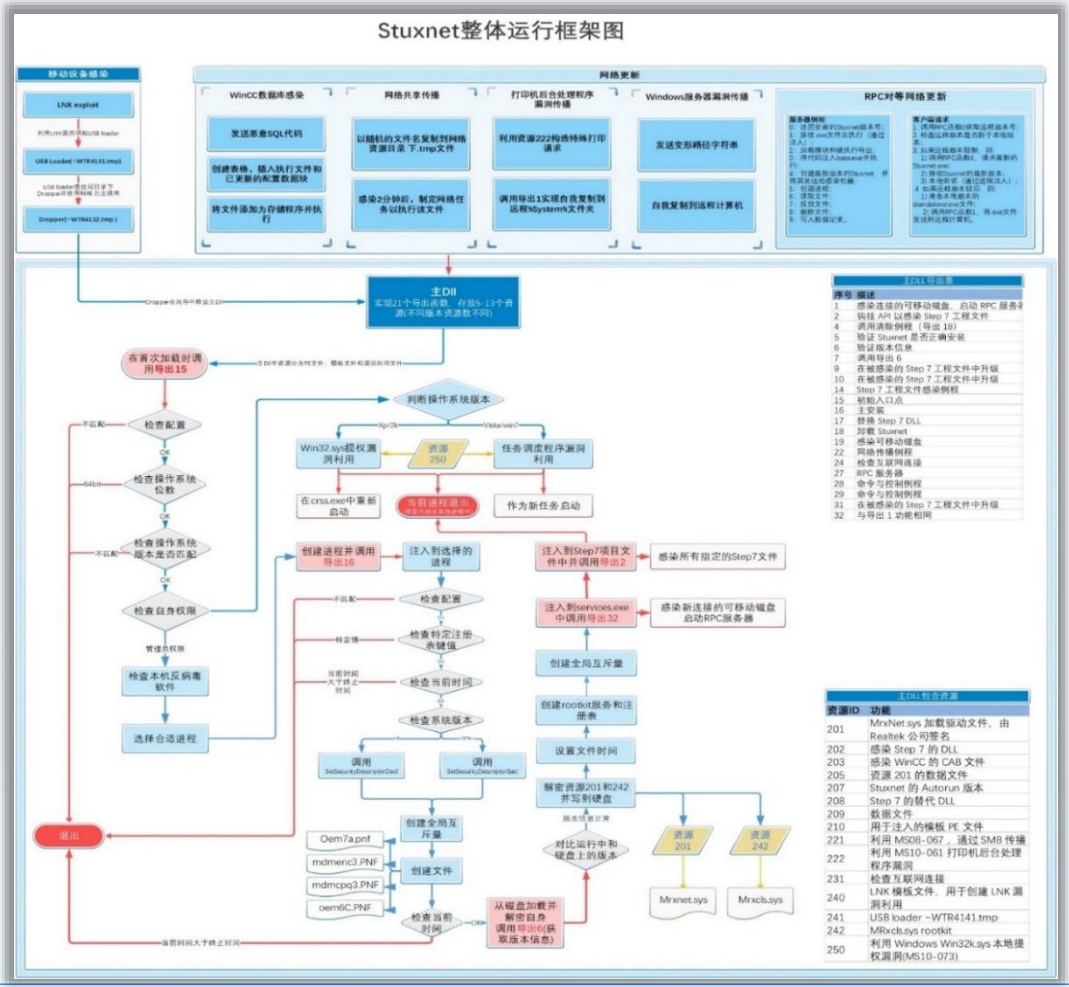
图片来源：https://www.mwrinfosecurity.com/our-thinking/observations-on-the-eastnets-breach-operation-notes/

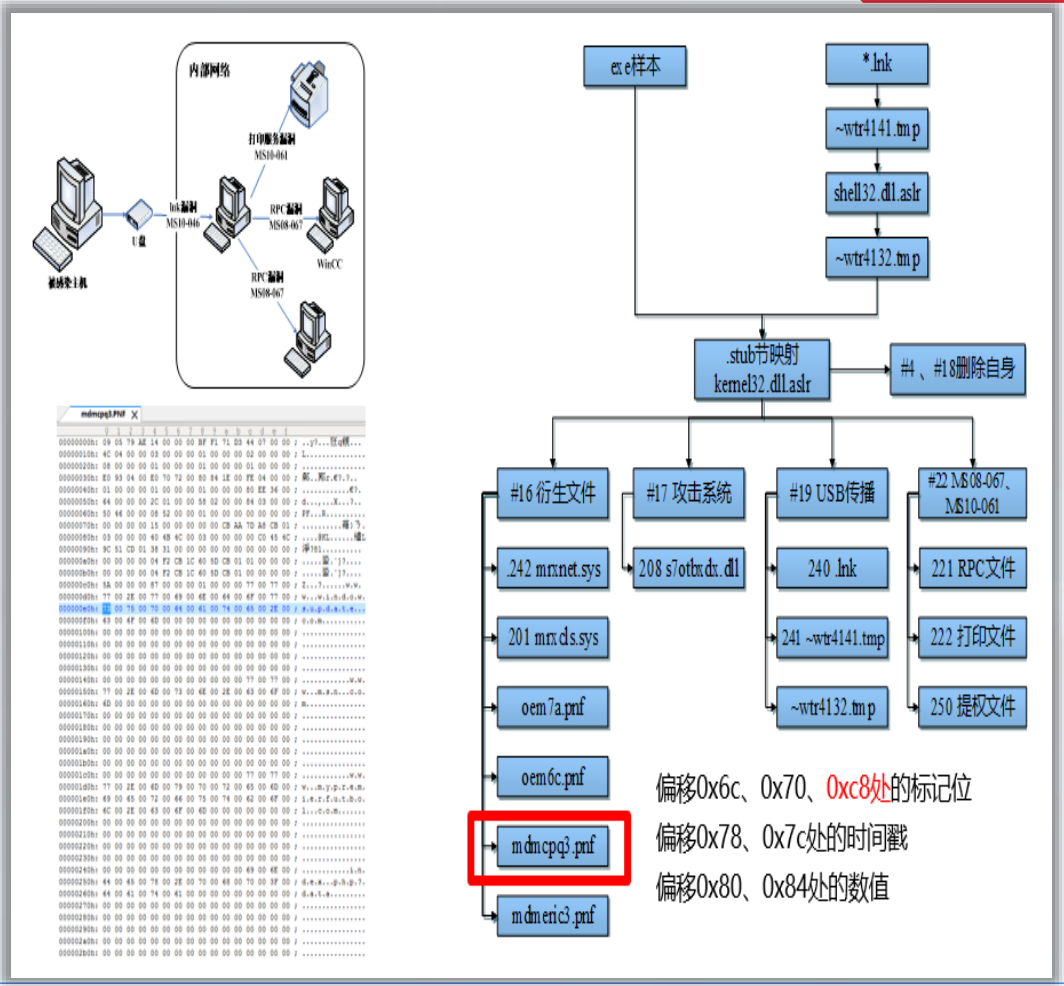
寒夜遠征

威胁框架：认知与实践

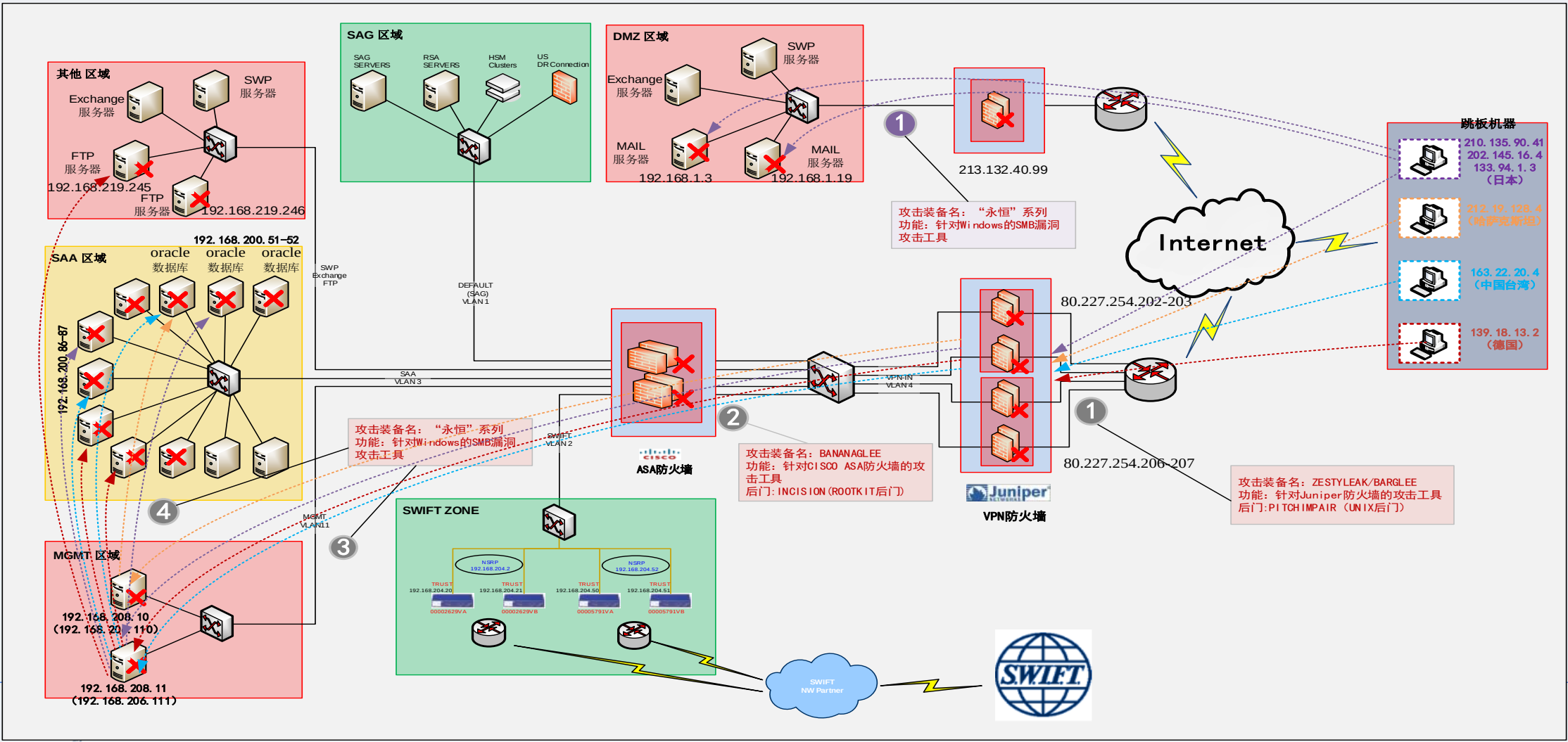
03 体系化支撑下的集成化武器作业与远程推进式作业

震网依靠集成化武器的严密逻辑进行无远程支撑隔离作业





“SWIFT”事件依靠体系化平台、模块化武器进行推进式远控作业



威胁框架如何解开“Michael之问”

Blog: SANS Digital Forensics and Incident Response Blog

24 Mar **2011**

Why Stuxnet Isn't APT

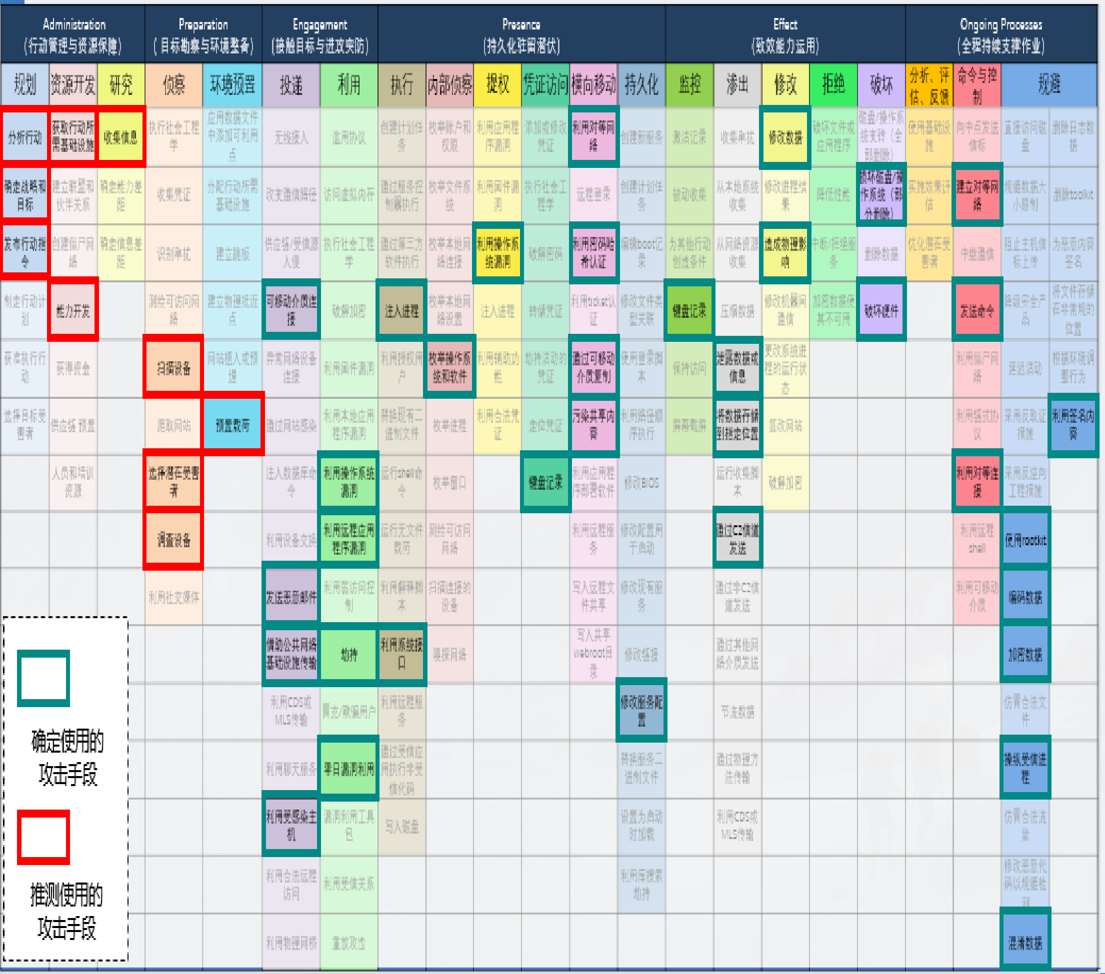
...or at least, shouldn't be considered as such...

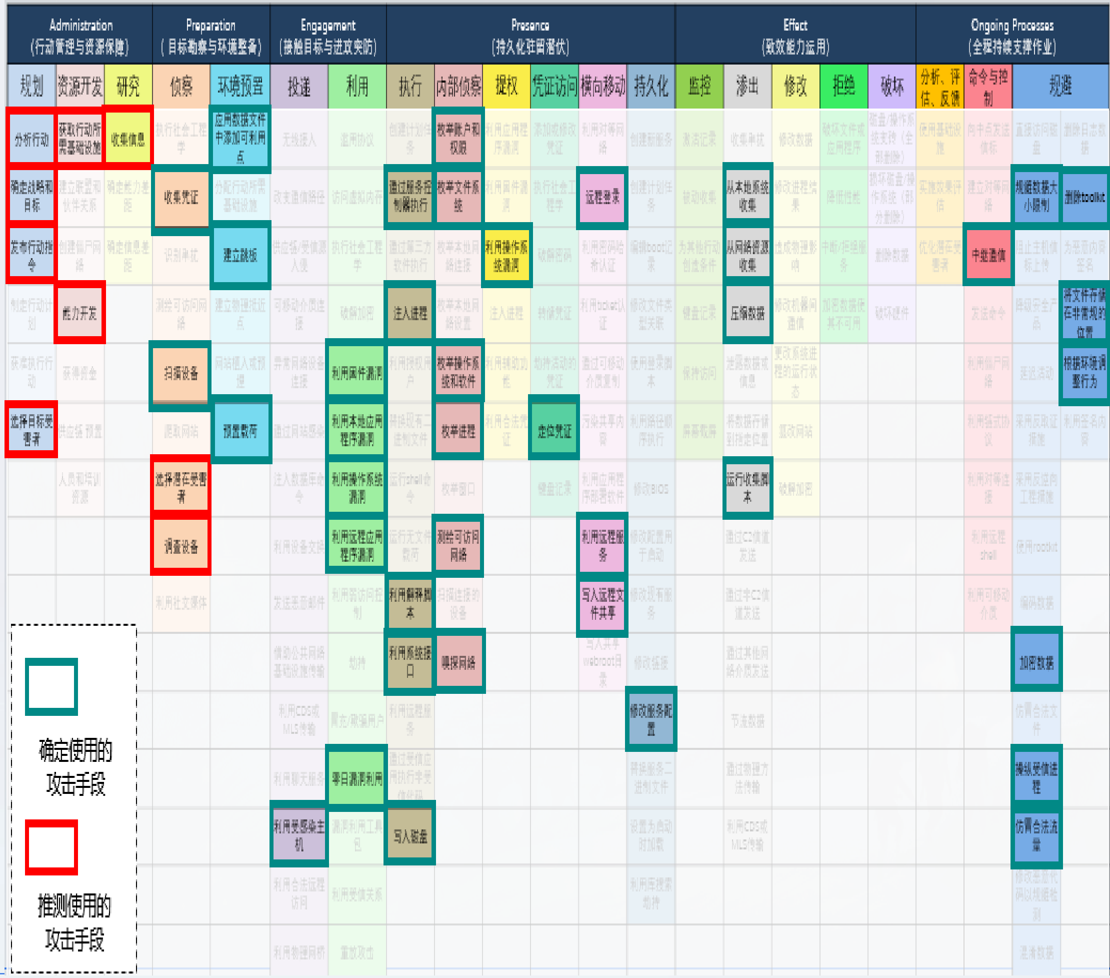
Stuxnet has become so buzz-worthy that I almost feel like an article relating it to "APT" is the epitome of anecdotal industry navel-gazing. Making a qualitative assessment of each can be a useful exercise in classifying and understanding the threat landscape, however. This in turn helps clarify risk, driving resource allocation, investment, and R&D. Even more important than the conclusions presented herein, I want to elucidate some of the analysis that goes into threat assessments so that others might be empowered to do the same. At the same time, do not interpret this as an exhaustive or 'correct' methodology, but rather a single case study.

So many unrelated conversations these days seem to drift toward the inclusion of Stuxnet that I'm beginning to see it like the invocation of a Hitler analogy in modern US political debates. There's a lot to be said about this event, to be sure, but I feel we can do much better in understanding similarities and differences in various threat landscapes, thus my initial motivation to write this article. The bottom line is that I feel we do both Stuxnet and APT a disservice by classifying the former into the latter, and worse yet, confuse what could otherwise be informed threat-oriented decisions on CND.

- 2014年3月，洛克希德·马丁公司的高级研究员Michael在博客上的震网事件的意图和能力两个方面进行了分析，提出了“Why Stuxnet Isn't APT？” 这一设问。
- Michael指出：“震网比普通的APT攻击更为复杂和高级”。“震网带来明显可感知后果的攻击，不符合APT攻击的持续隐蔽定向的特点。”
- 其观点是： APT攻击已经完全是CNE（网络情报利用）；而震网是一种军事行动，应归于CNA（计算机网络攻击）。
- 而站在整个威胁框架来看，震网的破坏与干扰活动均属于致效能力运用。

不同作业模式在威胁框架下对比





针对中东国家的军事行动和网络攻击行动的对比分析

	凋谢利刃与巴比伦行动（传统物理攻击伊拉克）	震网行动（网络空间攻击伊朗）	SWIFT事件（网络空间攻击中东服务商）
被攻击目标	伊拉克核反应堆	伊朗纳坦兹铀离心设施	中东SWIFT服务商EastNets
时间周期	1977-1981年	2006-2010年	2012-2013（不含准备时间）
人员投入	以色列空军、特工人员、伊朗空军、美国空军和情报机构	美、以情报和军情领域的软件和网络专家，工业控制和核武器的专家	美情报、银行业务、软件、网络安全攻防专家以及网络武器外包商
作战准备	多轮前期侦查和空袭，核反应堆情报	战场预置、病毒的传播和相关核设施情报	战场预置、业务系统设施和网络拓扑情报
各方装备投入	伊：2架F-4鬼怪式以12枚MK82减速炸弹-轰炸核反应堆假设工地；10架F-4袭击伊拉克H-3空军基地。 以：2架F-4E(S)-侦查任务；8架F-16A(美方提供)、4架F-15A、2架F-15B、16枚MK84炸弹-空袭反应堆 模拟搭建反应堆 特工人员暗杀伊拉克关键人员 美：战略卫星和情报、空中加油机	供应链攻击 特工情报作业 编制震网病毒 C2服务器 模拟搭建离心机和控制体系	全球跳板机 防火墙、VPN设备漏洞利用武器 Linux、Windows等端点漏洞利用武器 各类系统植入武器和植入物
前期成本	18个月模拟空袭训练，训练2架F-4鬼怪攻击坠毁，3名飞行员阵亡	跨越两位总统任期，经历了5年的持续开发和改进	前期情报和资产信息探测、借助已有项目成果，复用体系化武器作业
毁伤效果	反应堆被炸毁，吓阻了法国供应商继续提供服务，伊拉克核武器计划永久迟滞	导致大量离心机瘫痪，铀无法满足武器要求，几乎永久性迟滞了伊朗核武器计划	获取EastNets大量金融交易数据，掌握中东地区资金变动
效费比	打击快速，准备期长，耗资巨大，消耗大，行动复杂，风险高	周期长，耗资相对军事打击低，但更加精准、隐蔽，不确定性后果更低	超长周期，庞大资金和技术支持，可复用的体系化系统化作业流程

谢谢大家