在野0day揭秘

威胁情报感知发现apt攻击

边亮　　360追日团队

2018 ISC 互联网安全大会 中国·北京

Internet Security Conference 2018　Beijing·China

（原中国互联网安全大会）

目录

360追日团队（HELIOS TEAM）

专注APT等高级威胁的研究。

致力于发现和披露更多的APT组织或行动。

截至目前已发现三十多个APT组织。

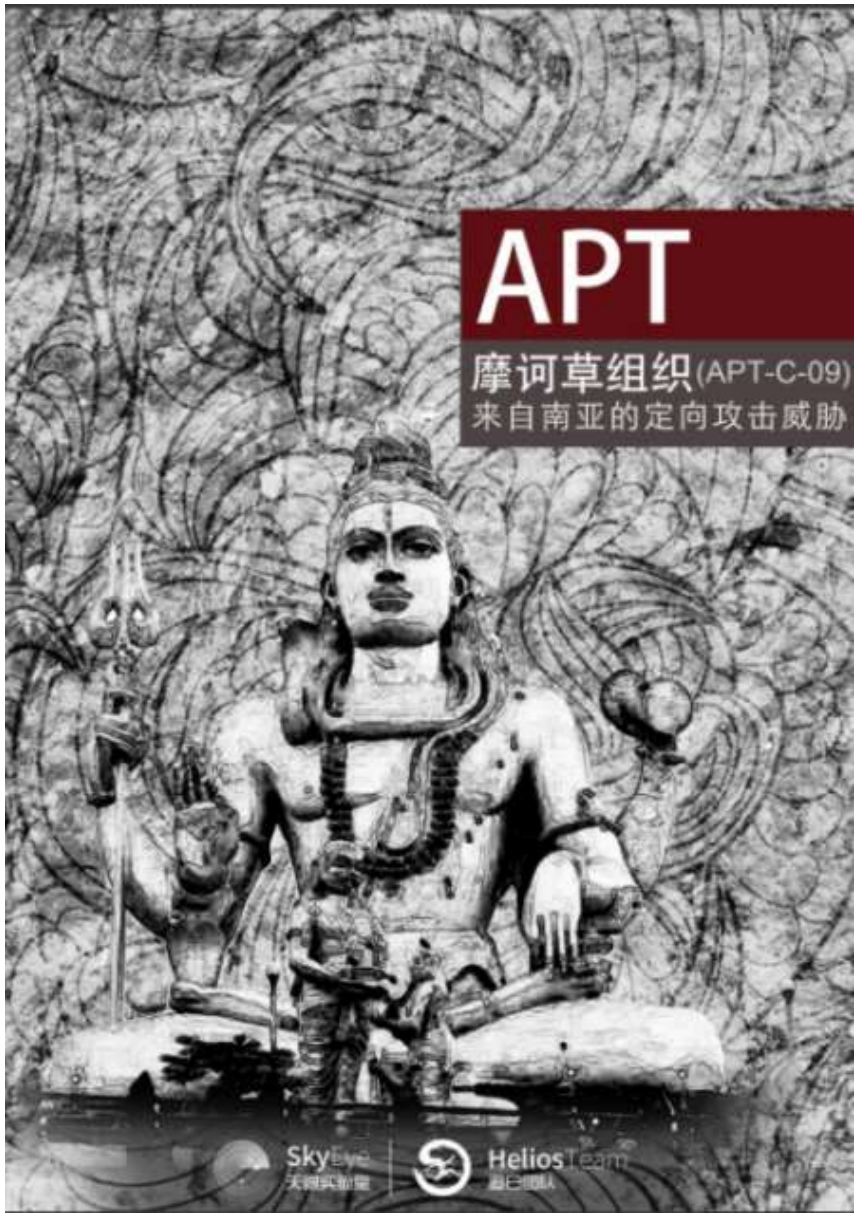
http://zhuiri.360.cn

监控和发现的APT

近期在野0DAY攻击回顾

2017年4月	CVE-2017-0199	HTA	In the Wild Attacks Leveraging HTA Handler	火眼
2017年6月	CVE-2017-0261/2/3	Word	EPS Processing Zero-Days Exploited by Multiple Threat Actors	火眼
2017年7月	CVE-2017-8464	Lnk	震网三代，360发布首个震网三代相关的隔离网络高级威胁攻击预警分析报告	360
2017年9月	CVE-2017-8759	Word	Zero-Day Used in the Wild to Distribute FINSPY	火眼
2017年10月	CVE-2017-11826	Word	360代表中国厂商全球独家捕获在野0day漏洞（CVE-2017-11826）	360
2017年10月	CVE-2017-11292	Flash	BlackOasis APT and new targeted attacks leveraging zero-day exploit	卡巴斯基
2017年12月	CVE-2018-0802	Word	360率先捕获噩梦公式二代漏洞，微软在2018年修复的首个在野0day漏洞	360
2017年12月	NULL	Web（国内某邮箱）	360捕获利用国内某邮箱漏洞攻击的在野0day	360
2018年2月	CVE-2018-4878	Flash	360国内首家捕获并分析预警，2018年第一个Adobe Flash零日漏洞在野攻击	360
2018年4月	CVE-2018-8174	Word & IE	360捕获全球首例利用浏览器0day漏洞的新型Office文档在野攻击-双杀漏洞	360
2018年6月	CVE-2018-5002	Flash	360在全球范围内率先捕获了使用Flash 0day漏洞的在野攻击	360
2018年7月	CVE-2018-8373	Word & IE	Use-after-free (UAF) Vulnerability CVE-2018-8373 in VBScript Engine Affects Internet Explorer to Run Shellcode	趋势科技

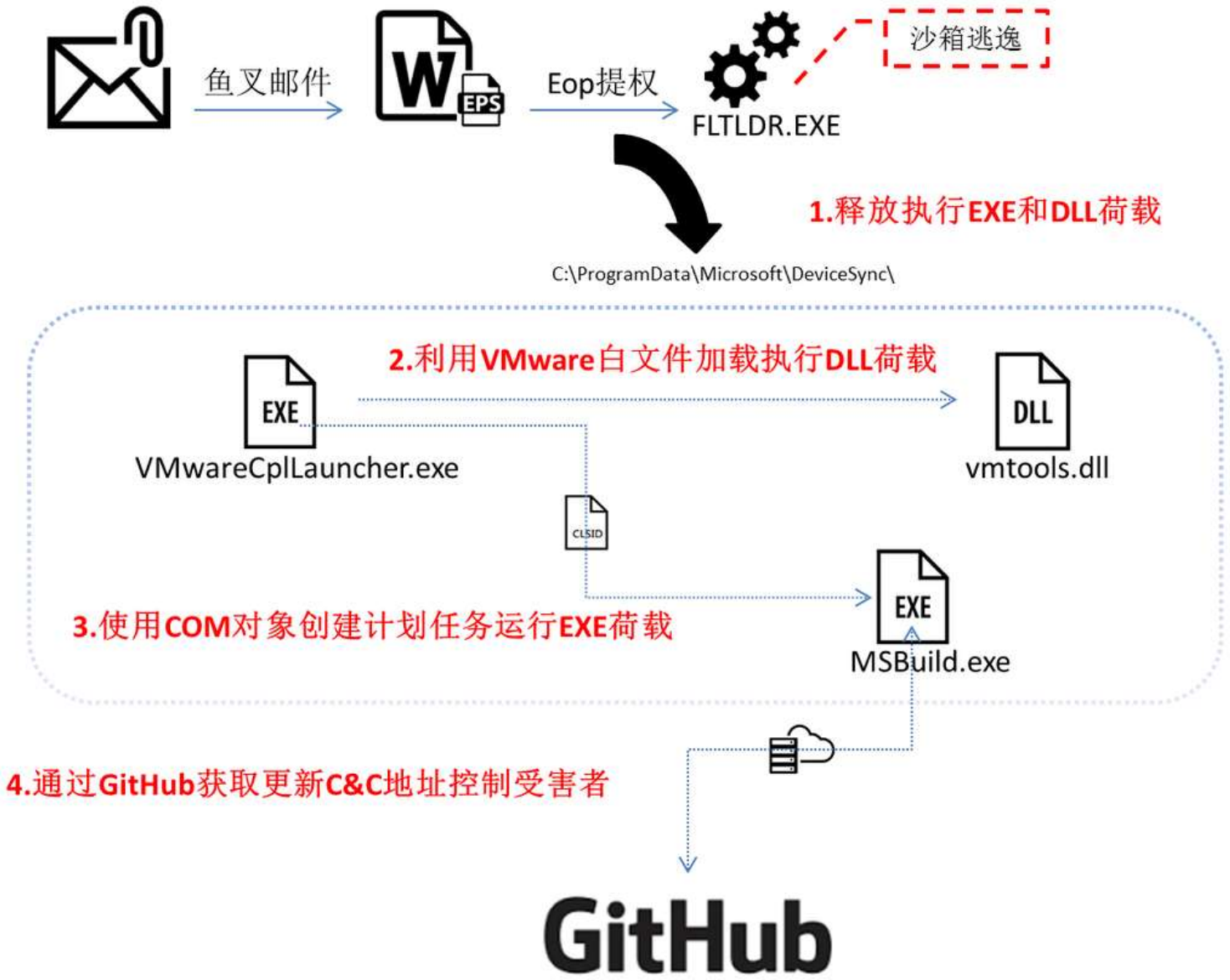
摩诃草组织



主要攻击手法

常用语言或语种	简体中文、英文
攻击前导	鱼叉邮件（二进制可执行文件） 鱼叉邮件（文档型漏洞文件） 鱼叉邮件（恶意网址） 水坑攻击 即时通讯工具 社交网络
0day利用的情况	CVE-2013-3906、CVE-2017-0199
漏洞利用种类	文档漏洞：CVE-2014-4114、CVE-2012-0158、CVE-2014-1761、CVE-2015-1641、CVE-2010-3333、CVE-2013-3906、CVE-2017-0261、CVE-2017-0262 Internet Explorer漏洞：CVE-2012-4792 Java漏洞：CVE-2012-0422
针对操作系统	Windows Mac OS X Android
横向移动	暂不披露
驻留机制	暂不披露
RAT种类	大类至少7种以上

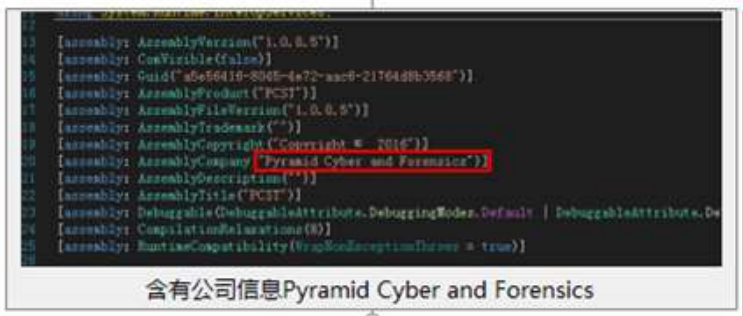
沙箱逃逸


鱼叉邮件
EPS
Eop提权
FLTLDR.EXE
沙箱逃逸
1.释放执行EXE和DLL荷载
C:\ProgramData\Microsoft\DeviceSync\
2.利用VMware白文件加载执行DLL荷载
EXE
VMwareCplLauncher.exe
DLL
vmtools.dll
CLSID
3.使用COM对象创建计划任务运行EXE荷载
EXE
MSBuild.exe
4.通过GitHub获取更新C&C地址控制受害者
GitHub

使用0DAY

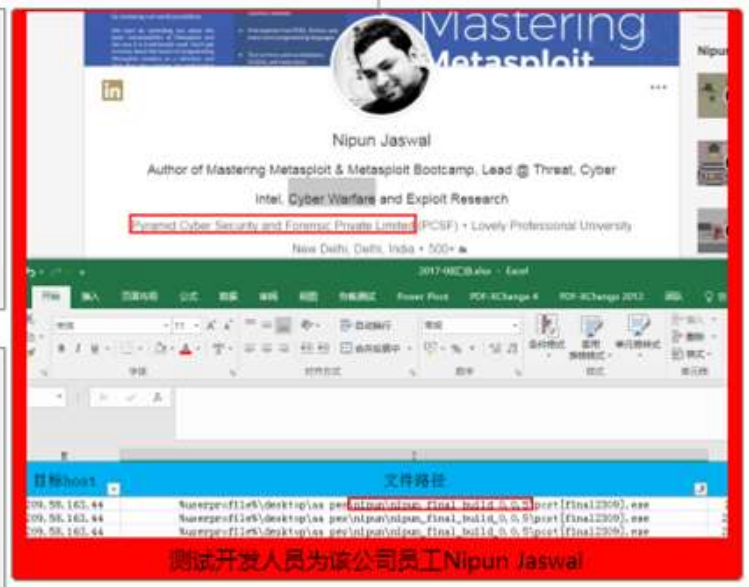
摩诃草针对360进行攻防测试

360追踪到主控制程序PCST.EXE



含有公司信息Pyramid Cyber and Forensics

该公司客户为印度中央调查局和印度国防部等情报单位



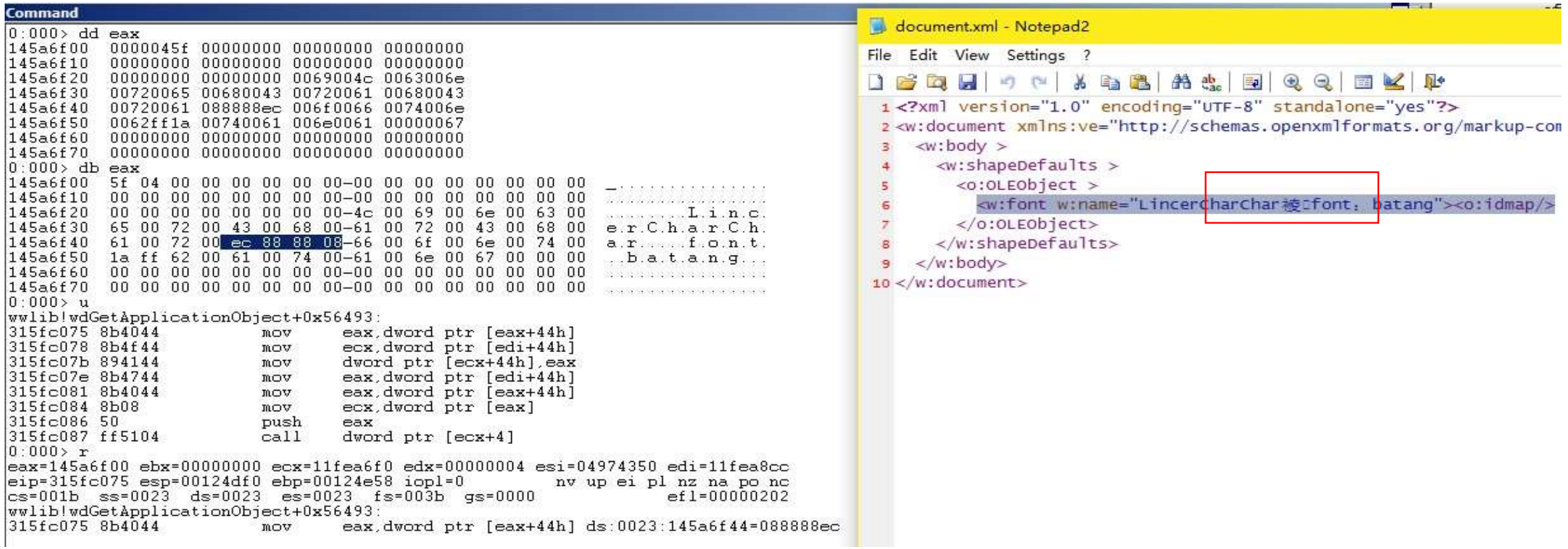
测试开发人员为该公司员工Nipun Jaswal

2016年11月-2017年8月-至今摩诃草组织使用C&C服务器

继续关联了同源的大量样本
a4fb5a6765cb8a30a8********
3fbb1267582acb7df5********
46416847e3f92d1ef********
...

CVE-2017-11826在野攻击

- 精心构造恶意的word文档标签和对应的属性值造成远程任意代码执行
- 与CVE-2015-1641漏洞有非常多的共同之处，是一例典型的类型混淆漏洞



CVE-2017-11826在野攻击

payload攻击流程

- 1.漏洞触发释放加载dll
- 2.上传IP地址和终端信息
- 3.下载payload压缩包
- 4.解压payload压缩包
  - xx.exe —— 白利用程序，带有运行参数的dll劫持漏洞
  - xx.dll —— 白利用加载dll，解密xx.ico数据在内存中运行
  - xx.ico —— 被加密的主体木马数据
- 5.上传窃密数据
  - 搜索如下文件上传
    .lfzmph/.txt/.doc/.docx/.pdf/.ppt/.pptx/.xls/.xlsx/.eml/.msg/.tif/.pmd/.gif/.jpg/.png/.bmp/.vsd/.csv/.xpg/.dwg/.pub/.png/.jpeg/.xps

噩梦公式二代在野攻击

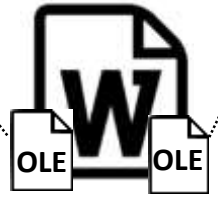
- 在“噩梦公式一代”的补丁中没有修复另一处拷贝字体FaceName时的栈溢出
- 攻击者构造恶意数据，覆盖了漏洞函数返回地址的后两个字节，然后将控制流导向了位于栈上的shellcode，巧妙绕过地址随机化保护。

```
LOGFONTA *__cdecl sub_21E39(LPCSTR lpLogfont, __int16 a2, LOGFONTA *lParam)
{
  LOGFONTA *result; // eax@7

  strcpy(lParam->lfFaceName, lpLogfont);
  lParam->lfCharSet = 1;
  EnumFontsA(hdc, lpLogfont, FMDFontProtoEnum, (LPARAM)lParam);
  lParam->lfWidth = 0;
  lParam->lfEscapement = 0;
  lParam->lfOrientation = 0;
  if ( a2 & 1 )
    lParam->lfWeight = 700;
  else
    lParam->lfWeight = 400;
  if ( a2 & 2 )
    lParam->lfItalic = 1;
  else
    lParam->lfItalic = 0;
  lParam->lfUnderline = 0;
  lParam->lfStrikeOut = 0;
  lParam->lfOutPrecision = 0;
  lParam->lfClipPrecision = 0;
  lParam->lfQuality = 0;
  result = lParam;
  lParam->lfPitchAndFamily = 0;
  return result;
}
```

噩梦公式二代在野攻击

CVE-2017-11882
Nday公式对象

CVE-2018-0802
0day公式对象



1. 样本包含两个公式OLE同时发起攻击
一个使nday漏洞公式对象
一个使用0day漏洞公式对象

2. 0day漏洞触发执行流
绕过公式编辑器进程的ASLR保护

Process	CPU	Privat...	PID	Description	Company Name	DEP	ASLR
csrss.exe	<...	3,220 K	504			n/a	n/a
wininit.exe	<...	2,108 K	860			n/a	n/a
csrss.exe	0.12	4,796 K	868			n/a	n/a
conhost.exe		2,228 K	3344	控制台窗口主机	Microsoft Corporation	Enabled (permen...	ASLR
winlogon.exe	<...	4,296 K	948			n/a	n/a
explorer.exe	0.20	107,176 K	2936	Windows 资源管理器	Microsoft Corporation	Enabled (permen...	ASLR
OUTLOOK.EXE	0.01	102,520 K	4408	Microsoft Outlook	Microsoft Corporation	Enabled (permen...	ASLR
POWERPNT.EXE	<...	57,052 K	8792	Microsoft Power...	Microsoft Corporation	Enabled (permen...	ASLR
WINWORD.EXE	<...	39,244 K	7728	Microsoft Word	Microsoft Corporation	Enabled (permen...	ASLR
EQNEDT32.EXE		2,696 K	6880	Microsoft Equat...	Design Science, Inc.	Disabled	ASLR
procexp64.exe	0.70	26,976 K	6928	Sysinternals Pr...	Sysinternals - www.sysin...	Enabled (permen...	ASLR

3.在野攻击按payload分为A、B两种样本
a.释放EXE文件至系统临时目录直接执行
b.释放DLL文件至Office插件目录随Word启动

A样本
%TMP%*.tmp

B样本
%APPDATA%\Microsoft\word\startup*.wll

国内某邮箱

- 2017年12月，360追日团队捕获到一批针对我国政府、贸易相关企业的针对性攻击
- 该组织最早从2016年5月起开始策划攻击，至今仍处于活跃状态
- 我们掌握了该组织使用的完整网络武器库、数据、源代码、攻击证据线索
- 该组织至少使用了国内某邮箱2个0day漏洞，其中一个0day在2017年底修补
- 在2018年初使用了该邮箱的另一个0day漏洞继续攻击
- 结合大数据平台进行追查溯源，关联到疑似实施APT攻击相关的公司、网络武器的开发者

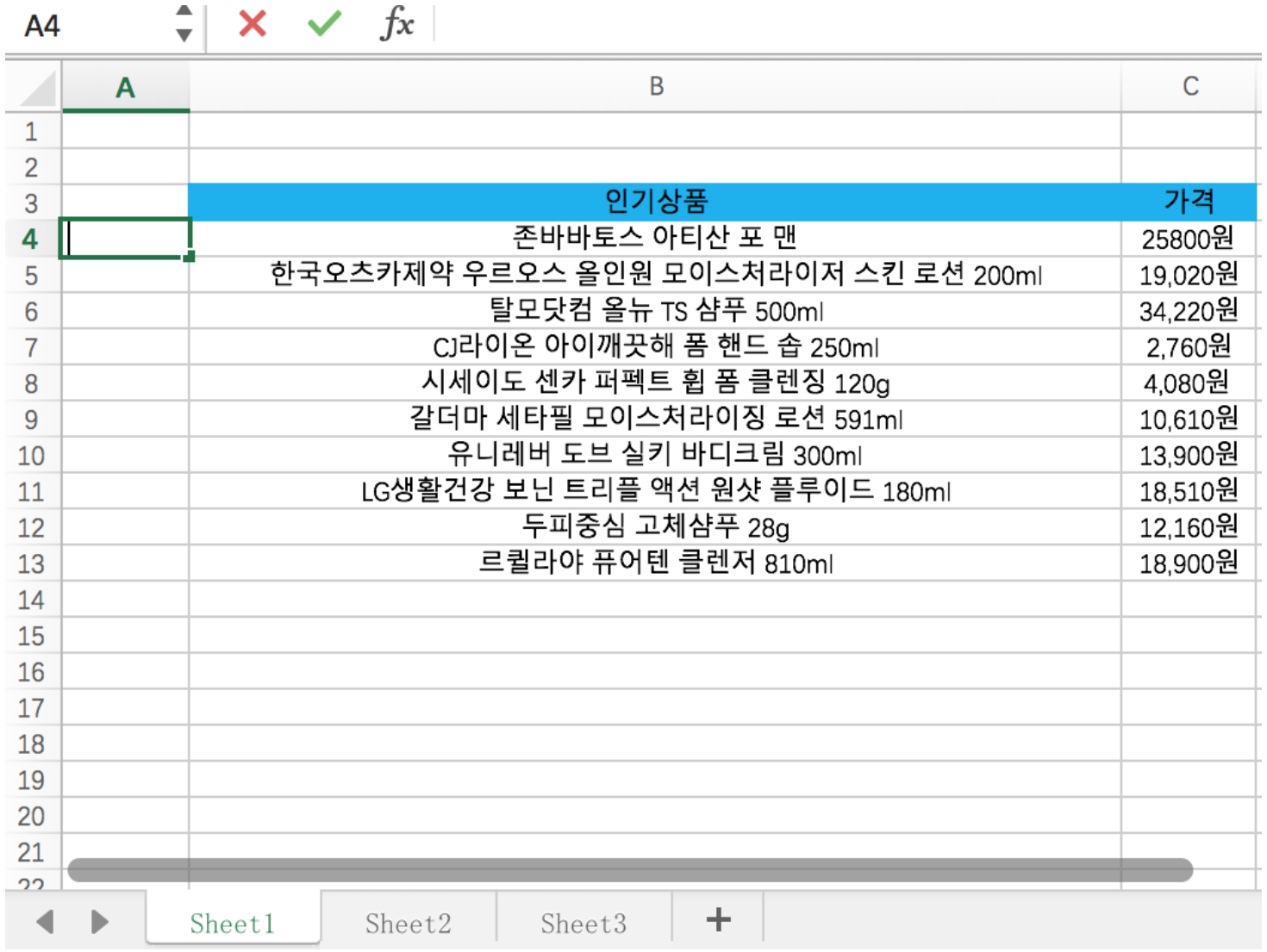
CVE-2018-4878在野攻击

- 漏洞存在于flash的DRMManager对象，相关的方法调用没有正确的处理导致UAF（Use-After-Free）漏洞
- 通过修改ByteArray对象的Length可以完成任意内存读写执行，执行最终的shellcode代码

```
49      public function method_3() : void
50      {
51          var §\x19§:* = null;
52          var data14:* = null;
53          §\x19§ = PSDK.pSDK;
54          data14 = §\x19§.createDispatcher();
55          this.var_15 = §\x19§.createMediaPlayer(data14);
56          this.var_16 = new class_8();
57          this.var_15.drmManager.initialize(this.var_16);
58          this.var_16 = null;
59      }
```

```
public function flash25() : void
{
    this.var_17 = new class_7();
    this.var_17.length = 512;
    if(this.var_13.a14 != 0)
    {
        for(var §\x1e\x0b§:int = 0; §\x1e\x0b§ < 5; §\x1e\x0b§ ++)
        {
            this.var_13.a32 = this.var_13.a14 + 8 * §\x1e\x0b§ + 7;
            this.var_17.flash26(§\x1e\x0b§ * 2 + 1,this.var_17.flash25());
        }
        this.var_17.a11 = 0;
        this.var_18 = this.var_13.a14;
```

CVE-2018-4878在野攻击



A4

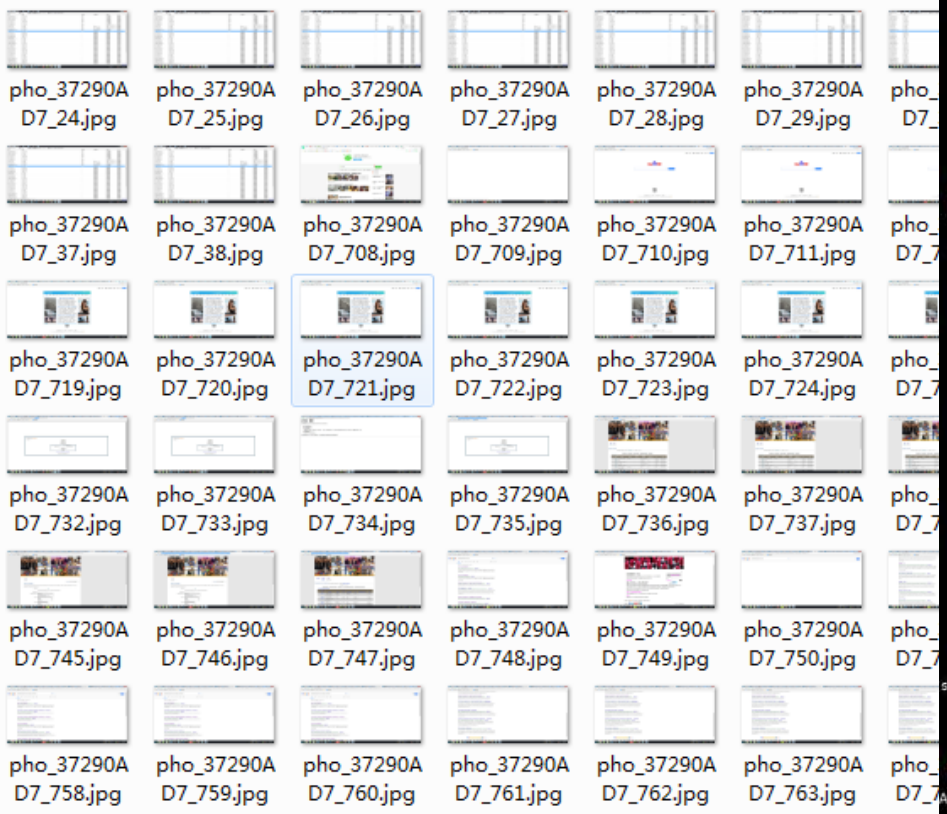
	A	B	C
1			
2			
3		인기상품	가격
4		존바바토스 아티산 포 맨	25800원
5		한국오츠카제약 우르오스 올인원 모이스처라이저 스킨 로션 200ml	19,020원
6		탈모닷컴 올뉴 TS 샴푸 500ml	34,220원
7		CJ라이온 아이깨끗해 폼 핸드 솝 250ml	2,760원
8		시세이도 센카 퍼펙트 휩 폼 클렌징 120g	4,080원
9		갈더마 세타필 모이스처라이징 로션 591ml	10,610원
10		유니레버 도브 실키 바디크림 300ml	13,900원
11		LG생활건강 보닌 트리플 액션 원샷 플루이드 180ml	18,510원
12		두피중심 고체샴푸 28g	12,160원
13		르퀼라야 퓨어텐 클렌저 810ml	18,900원
14			
15			
16			
17			
18			
19			
20			
21			

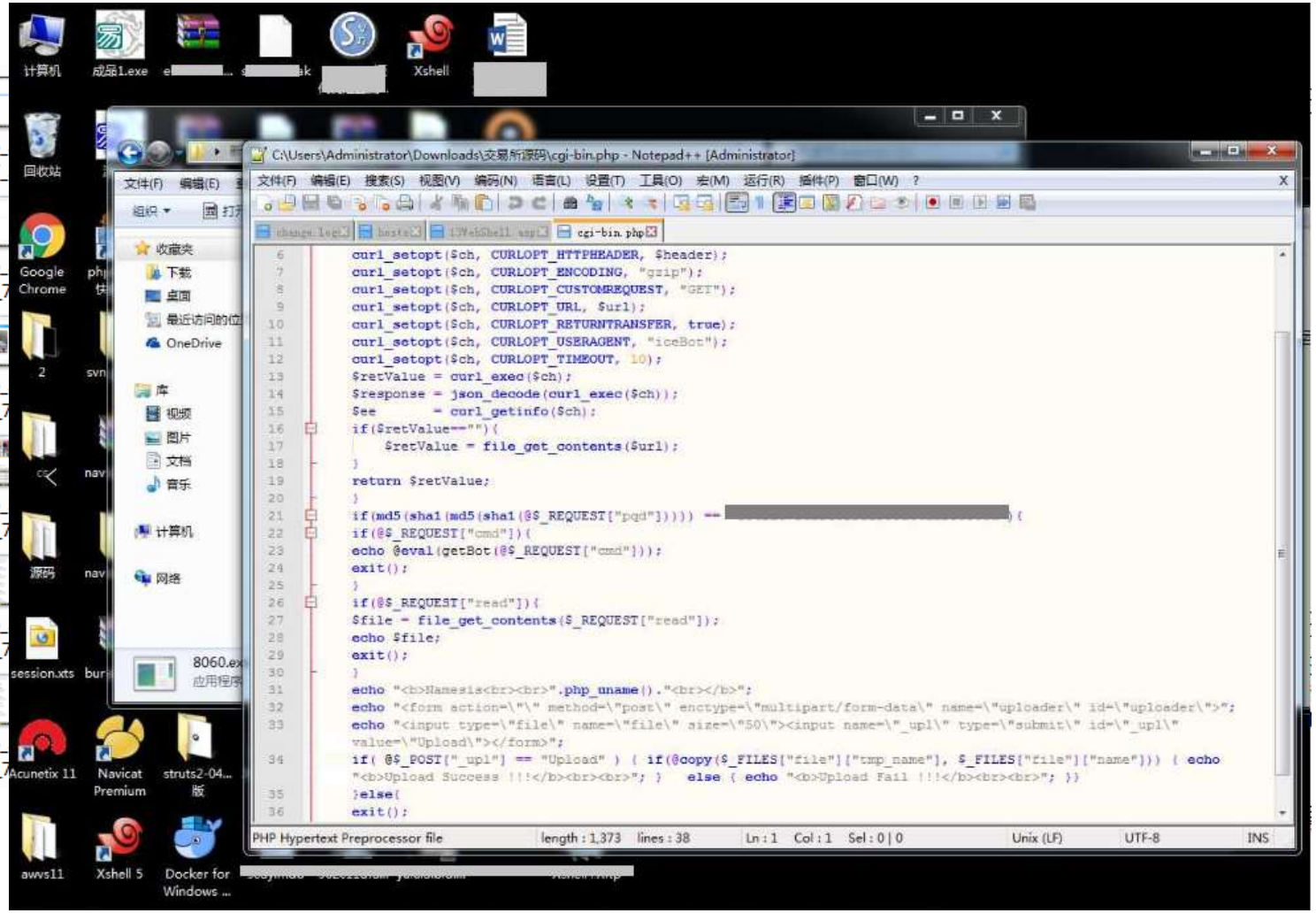
Sheet1 Sheet2 Sheet3

CVE-2018-4878在野攻击

109440	045B869B 64EB3A95 68F1807B FFE06201 F3E6DFDB A8F8A807 342F0A04 17CB7BE2	[..d.:.h..{….b ……. 4/ .{.
109472	5BF6DE02 5D58695D 150BC6BA A2A7FBA8 45FF30D2 5B941D82 A8929E4E FE513034	[..]Xi] ……E…0.[. ╗...N™Q04
109504	C1F24433 FF075E5E 0424FF01 3D72B7AD 718E427C 58FF1545 00000002 00000000	..D3… ^^ $… =r..q.B\X… E
109536	00687474 703A2F2F 7777772E 64796C62 6F696C65 722E636F 2E6B722F 61646D69	http://www.dylboiler.co.kr/admi
109568	6E63656E 7465722F 66696C65 732F626F 61642F34 2F6D616E 61676572 2E706870	ncenter/files/boad/4/manager.php
109600	160E0100 01006C6F 61647377 665F5357 4642436C 61737300 BF14E40A 00000100	loadswf_SWFBClass . .
109632	00006C6F 61647377 66001000 2E000364 0A00007D 076C6F61 64737766 0031463A	loadswf . d } loadswf 1F:
109664	5C776F72 6B5C666C 6173685C 6F626675 73636174 696F6E5C 6C6F6164 7377665C	\work\flash\obfuscation\loadswf\
109696	7372633B 3B6C6F61 64737766 2E617311 6C6F6164 7377665F 53574642 436C6173	src;;loadswf.as loadswf_SWFBClas
109728	73095357 4642436C 6173730D 6C6F6164 7377665F 4D795552 4C054D79 55524C09	s SWFBClass loadswf_MyURL MyURL
109760	54657874 4669656C 640A666C 6173682E 74657874 06747874 666C640A 55524C52	TextField flash.text txtfld URLR
109792	65717565 73740966 6C617368 2E6E6574 0B6D7955 726C5265 71657374 0955524C	equest flash.net myUrlReqest URL
109824	4C6F6164 65720B6D 7955726C 4C6F6164 65720577 69647468 06686569 67687408	Loader myUrlLoader width height
109856	61646443 68696C64 05457665 6E740C66 6C617368 2E657665 6E747308 434F4D50	addChild Event flash.events COMP
109888	4C455445 07446563 72697074 10616464 4576656E 744C6973 74656E65 720C494F	LETE Decript addEventListener IO
109920	4572726F 72457665 6E740849 4F5F4552 524F520F 4F6E494F 4572726F 7248616E	ErrorEvent IO_ERROR OnIOErrorHan
109952	646C6512 53656375 72697479 4572726F 72457665 6E740E53 45435552 4954595F	dle SecurityErrorEvent SECURITY_
109984	4552524F 52154F6E 53656375 72697479 4572726F 7248616E 646C6509 42797465	ERROR OnSecurityErrorHandle Byte
110016	41727261 790B666C 6173682E 7574696C 73076269 6E446174 61135365 6E644765	Array flash.utils binData SendGe
110048	74537766 4B657952 65716573 740F6C6F 61647377 662F6C6F 61647377 66067377	tSwfKeyReqest loadswf/loadswf sw
110080	665F6964 06737472 44626706 6D795F75 726C0C43 61706162 696C6974 6965730C	f_id strDbg my_url Capabilities
110112	666C6173 682E7379 7374656D 0A697344 65627567 67657202 2D440B73 7A5F7377	flash.system isDebugger -D sz_sw
110144	665F6865 61640669 645F6C65 6E0A7772 69746542 79746573 0A537472 696E6755	f_head id_len writeBytes StringU
110176	74696C08 6D782E75 74696C73 08746F53 7472696E 67047472 696D0375 726C043F	til mx.utils toString trim url ?

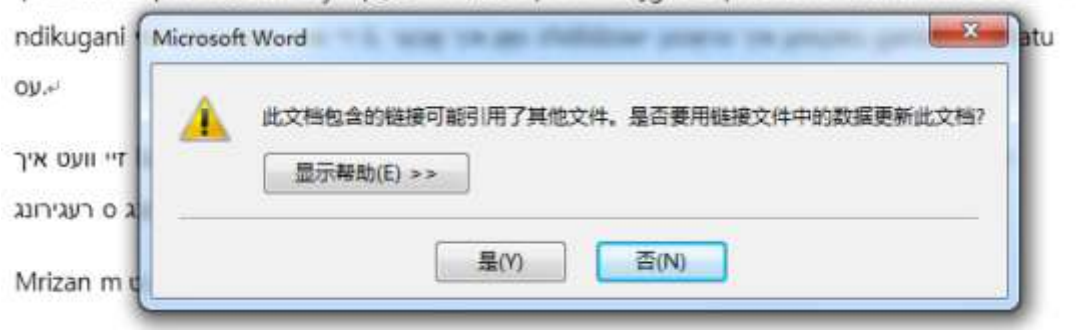
CVE-2018-4878在野攻击





双杀漏洞在野攻击

- 利用Office的OLE autolink漏洞利用方式嵌入远程的恶意网页

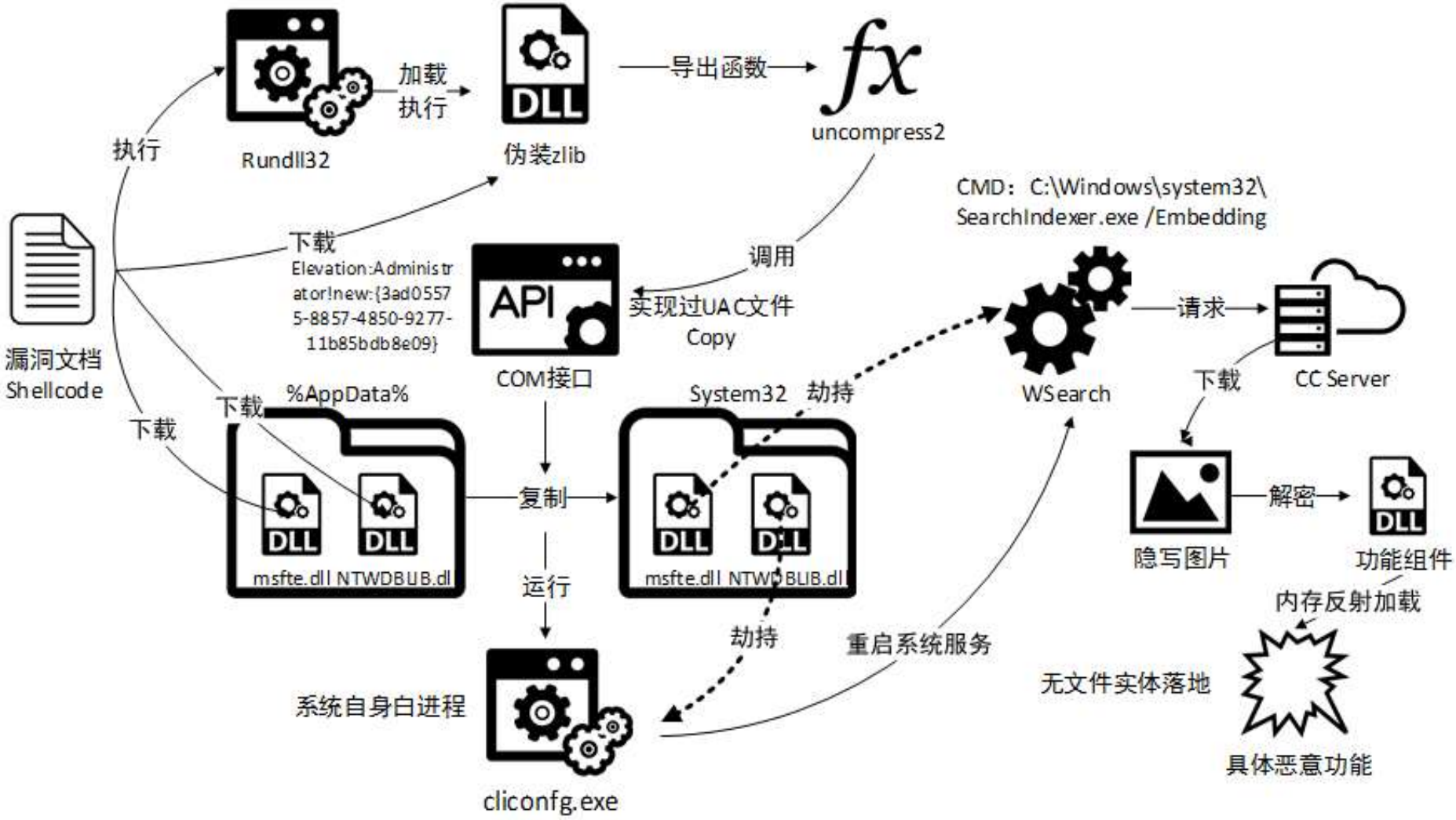


- 利用Vbscript漏洞，精心构造的SafeArray结构体头信息，伪造了一个可以读写任意地址的数组类型，最终绕过安全限制执行shellcode。

```
lIlIIl=Unescape("%u0001%u0880%u0001%u0000%u0000%u0000%u0000%u0000" & _
"%uffff%u7fff%u0000%u0000")
```

```
typedef struct tagSAFEARRAY {
USHORT cDims; // cDims = 0001
USHORT fFeatures; fFeatures =0x0880
ULONG cbElements; //一个元素所占字节（1个字节）
ULONG cLocks;
PVOID pvData; //数据的Buffer从0x0开始
SAFEARRAYBOUND rgsabound[1];
} SAFEARRAY, *LPSAFEARRAY;
```

双杀漏洞在野攻击


Rundll32
加载
执行
伪装zlib
导出函数
uncompress2
执行
下载
Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
调用
实现过UAC文件
Copy
漏洞文档
Shellcode
API
COM接口
CMD：C:\Windows\system32\SearchIndexer.exe /Embedding
WSearch
请求
CC Server
下载
下载
%AppData%
System32
劫持
msfte.dll NTWDBLIB.dll
复制
运行
劫持
重启系统服务
隐写图片
解密
功能组件
内存反射加载
无文件实体落地
具体恶意功能
系统自身白进程
cliconfg.exe

CVE-2018-5002在野攻击

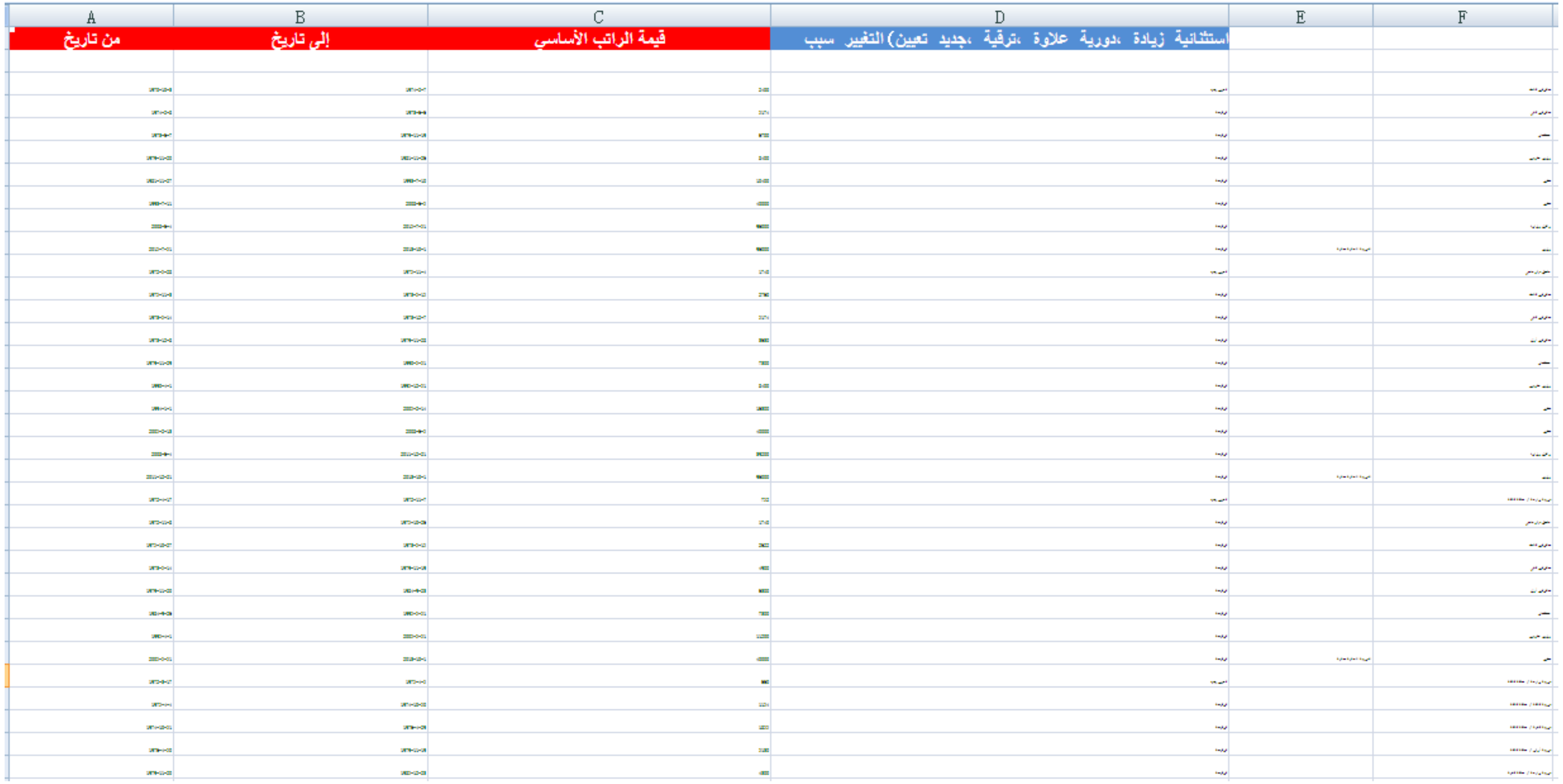
- 解释器在处理try catch语句时没有正确的处理好异常的作用域
- 没有对catch语句块中的字节码做检查
- 攻击者通过在catch语句块中使用getlocal，setlocal指令来实现对栈上任意地址读写
- 攻击者通过交换栈上的2个对象指针来将漏洞转为类型混淆问题完成攻击

```
1  package
2  {
3      import avm2.intrinsics.memory.li8;
4
5      public class class_6
6      {
7          {
8              try{
9              }
10             catch(e:Error)
11             {
12                 var _loc139_:int = 1094795585;
13                 return;
14             }
15             li8(123456);
16         }
17
18         public function class_6(){
19             super();
20         }
21     }
22 }
```

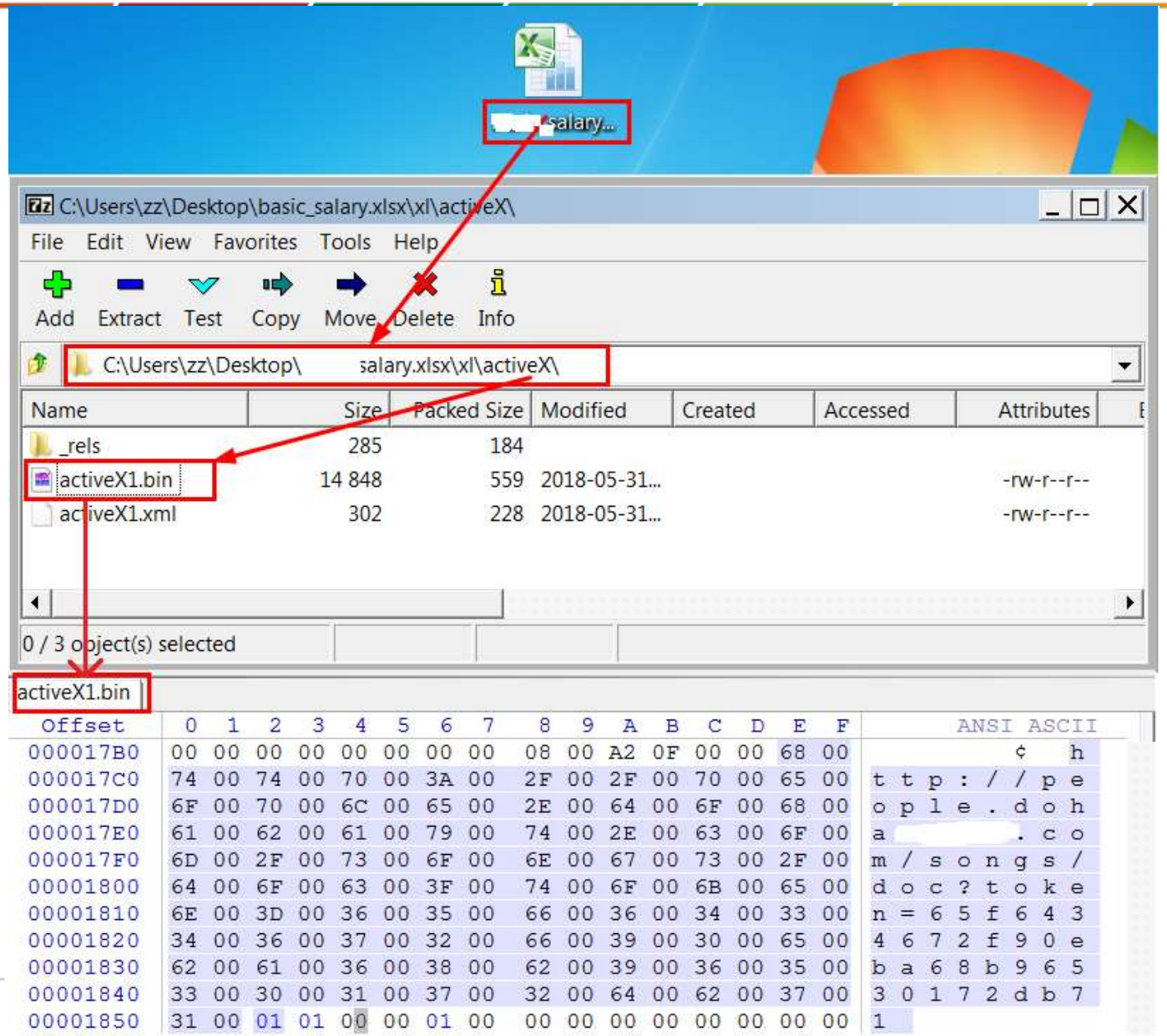
```
package
{
   import avm2.intrinsics.memory.li8;

   public class class_6
   {

      {
         li8(123456);
      }

      public function class_6()
      {
         super();
      }
   }
}
```

```
6  maxstack 3
7  localcount 2
8  initscopedepth 3
9  maxscopedepth 6
10 try from ofs0000 to ofs0004 ta
11
12 code
13 ofs0000:jump ofs0024
14 ofs0004:getlocal_0
15 pushscope
16 newcatch 0
17 dup
18 setlocal_1
19 dup
20 pushscope
21 swap
22 setslot 1
23 getlocal 449
24 setlocal_0
25 getlocal 448
26 setlocal 449
27 getlocal_0
28 setlocal 448
29 popscope
30 kill 1
31 jump ofs0028
32 ofs0024:pushint 123456
33 li8
34 pop
35 ofs0028:returnvoid
```

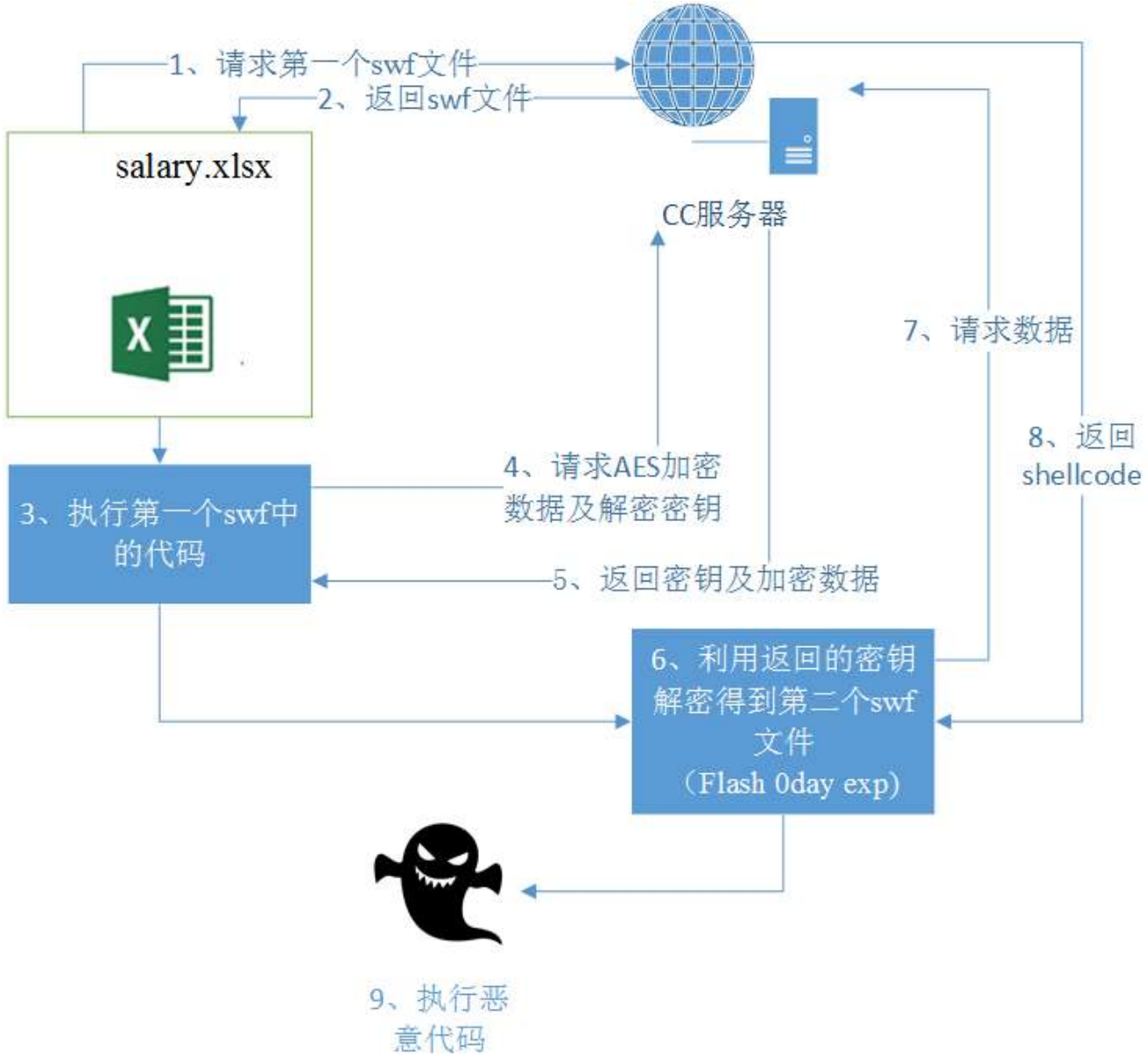
CVE-2018-5002在野攻击



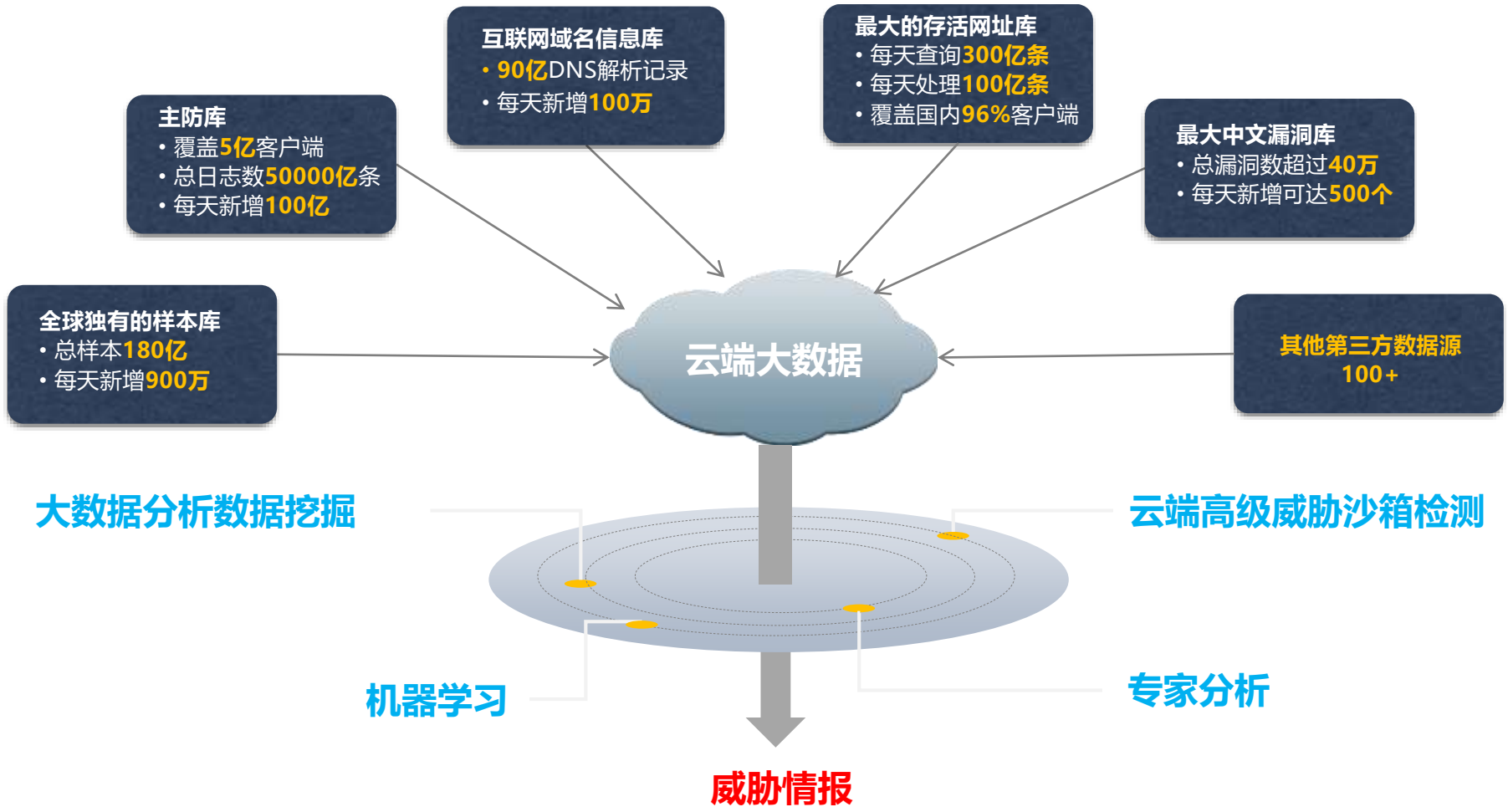
CVE-2018-5002在野攻击



CVE-2018-5002在野攻击



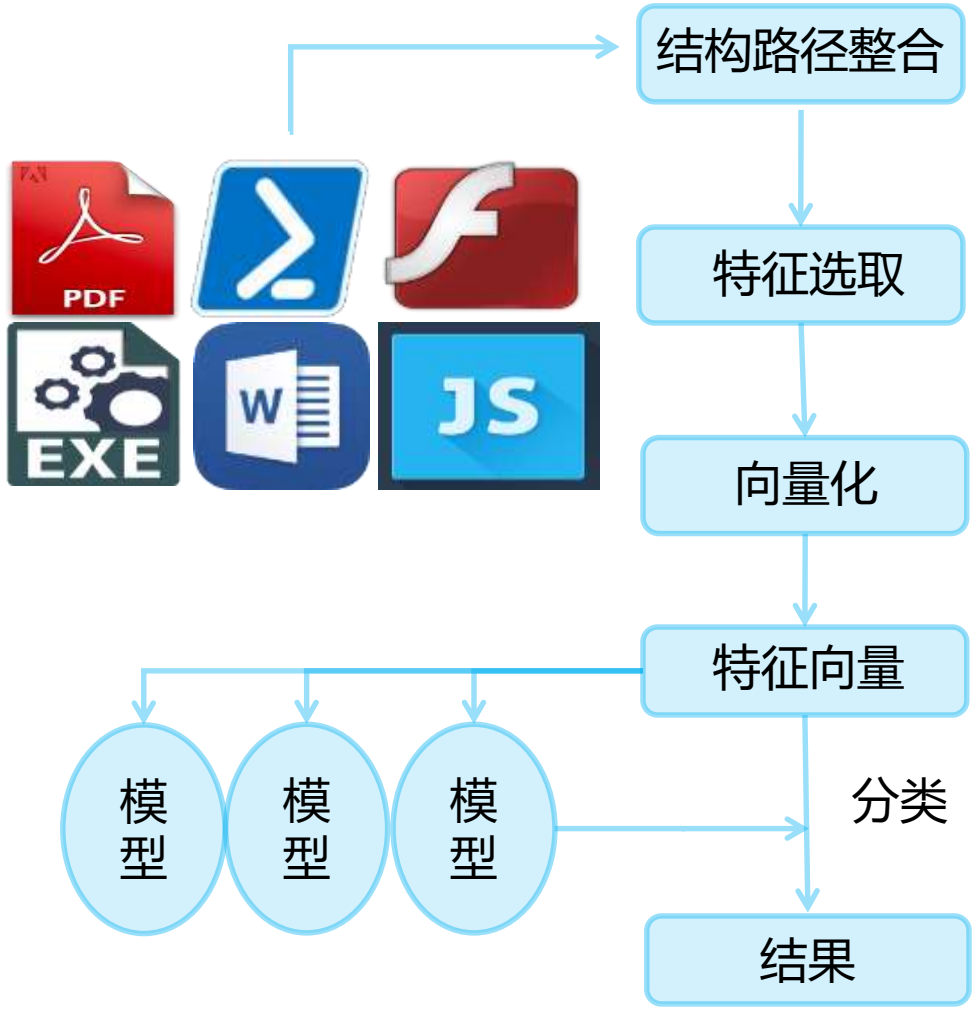
基于大数据的威胁情报


互联网域名信息库
• 90亿DNS解析记录
• 每天新增100万
最大的存活网址库
• 每天查询300亿条
• 每天处理100亿条
• 覆盖国内96%客户端
主防库
• 覆盖5亿客户端
• 总日志数50000亿条
• 每天新增100亿
最大中文漏洞库
• 总漏洞数超过40万
• 每天新增可达500个
全球独有的样本库
• 总样本180亿
• 每天新增900万
云端大数据
其他第三方数据源
100+
大数据分析数据挖掘
云端高级威胁沙箱检测
机器学习
专家分析
威胁情报

大数据存储和搜索技术

- 专门针对大数据（**千万亿**）做特殊算法优化，单表规模**10000亿**
- 对现有Map/Reduce任务完全兼容
- 分词算法灵活，完全适配安全各领域的数据
- 秒级查询响应
- 索引数据写入速度达100万QPS

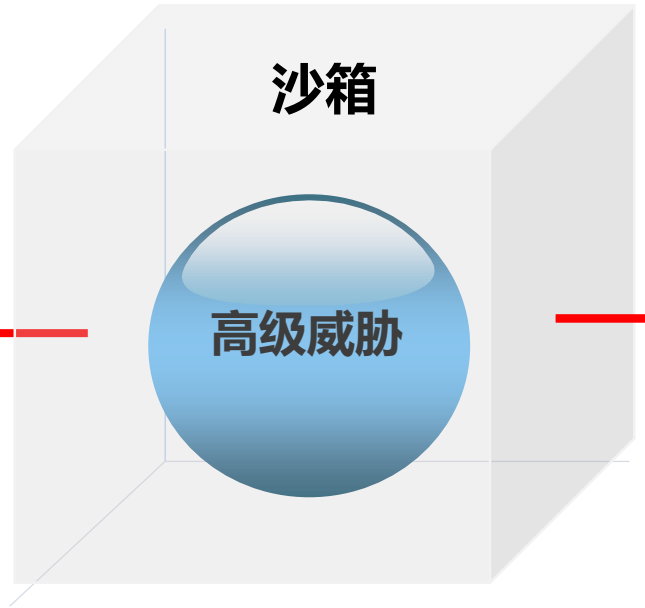
机器学习自动分类和识别



高级威胁沙箱检测技术

漏洞利用监控

- 是否在堆栈上执行了代码
- 是否在数据区执行代码
- 是否进行了内存布局
- 是否调用了其他函数指令
- ....



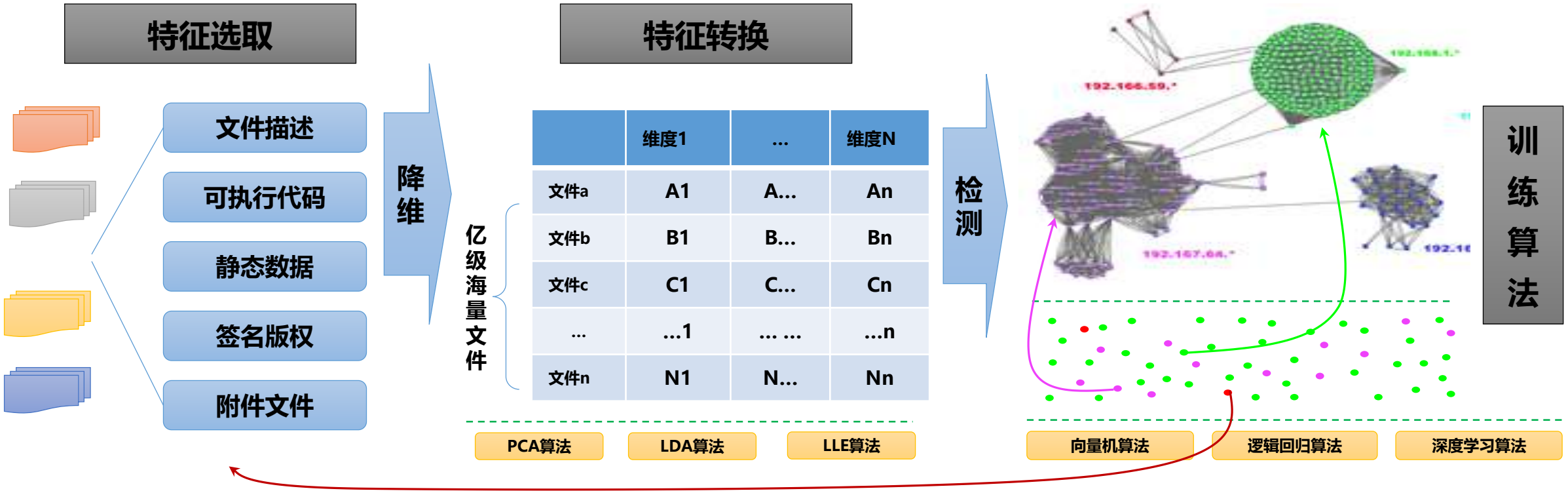
恶意行为监控

- 是否释放可以文件
- 是否创建可以进程
- 是否修改注册表
- ....

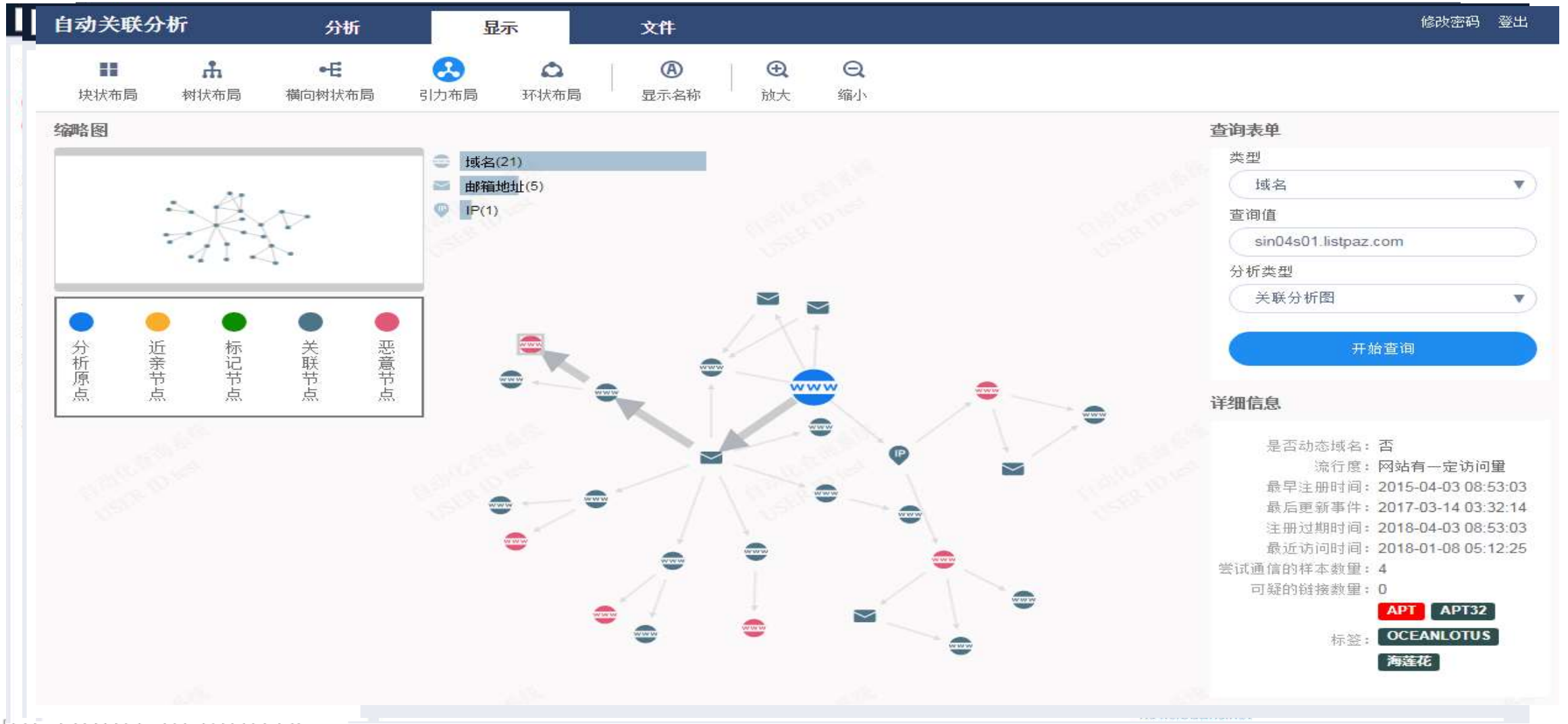
网络行为监控

- 是否发起对外链接
- 是否启用HTTP或FTP
- 是否使用DNS Beacon
- ....

机器学习快速查杀和回扫



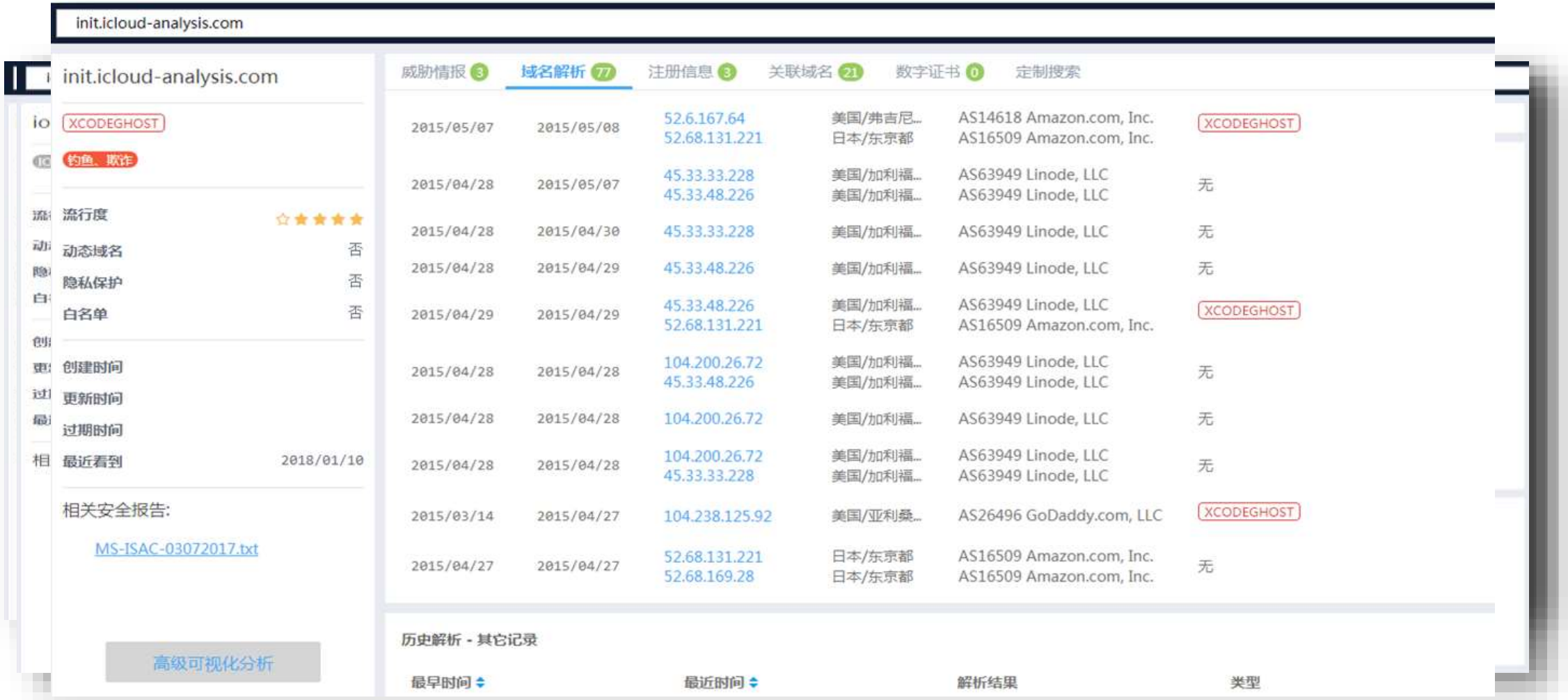
威胁分析数据平台


自动关联分析
分析
显示
文件
修改密码
登出
块状布局
树状布局
横向树状布局
引力布局
环状布局
显示名称
放大
缩小
缩略图
域名(21)
邮箱地址(5)
IP(1)
分析原点
近亲节点
标记节点
关联节点
恶意节点
查询表单
类型
域名
查询值
sin04s01.listpaz.com
分析类型
关联分析图
开始查询
详细信息
是否动态域名：否
流行度：网站有一定访问量
最早注册时间：2015-04-03 08:53:03
最后更新事件：2017-03-14 03:32:14
注册过期时间：2018-04-03 08:53:03
最近访问时间：2018-01-08 05:12:25
尝试通信的样本数量：4
可疑的链接数量：0
APT
APT32
标签：
OCEANLOTUS
海莲花

安全事件的定性


aaa.xxxatat456.com
威胁情报
域名解析
注册信息
关联域名
定制搜索
开源情报
恶意家族
恶意类型
僵尸网络
风险等级
影响平台
Linux
其他名称
描述
LDX（Linux Xor DDoS）是一种运行于Linux系统下的木马程序，由C++编辑而成，使用rootkit技术。该木马中大量使用异或加密算法。受此恶意代码感染的系统连接至C&C服务器获得目标列表并进行DDoS攻击，90%攻击目标在亚洲。
细节：
1.特点：
（1）异或加密算法：样本和C&C通信中大量使用异或加密算法，密文是由异或明文对一个16字节的密钥生成，所有的C&C消息被异或加密，但不包括消息头部。样本中只有两处不同的二进制解密代码，解密代码固定。
（2）C&C通信：基于TCP协议，大多数使用80端口，数据包头格式固定。
（3）DDoS攻击：使用最多的攻击类型为syn_flood类型，攻击时前期为syn/dns flood类型，后期跟有tcp_ack_flood类型。
（4）更新：下载和执行任意的二进制文件，更新自身。
2.传播方式：
通过嵌入式设备，利用计算机的SSH服务获得目标计算机的root访问权限。获得安全证书并登入后，攻击者运行shell脚本下载木马程序。
参考链接
https://www.yumpu.com/en/document/view/54673736/the-linux-xor-ddos-botnets/37
http://thehackernews.com/2015/09/xor-ddos-attack.html
http://www.securityweek.com/linux-xor-ddos-botnet-flexes-muscles-150-gbps-attacks
IP

安全事件的溯源


init.icloud-analysis.com
init.icloud-analysis.com
XCODEGHOST
钓鱼、欺诈
流行度
动态域名 否
隐私保护 否
白名单 否
创建时间
更新时间
过期时间
最近看到 2018/01/10
相关安全报告:
MS-ISAC-03072017.txt
高级可视化分析
威胁情报 3
域名解析 77
注册信息 3
关联域名 21
数字证书 0
定制搜索
2015/05/07 2015/05/08 52.6.167.64 52.68.131.221 美国/弗吉尼... 日本/东京都 AS14618 Amazon.com, Inc. AS16509 Amazon.com, Inc. XCODEGHOST
2015/04/28 2015/05/07 45.33.33.228 45.33.48.226 美国/加利福... 美国/加利福... AS63949 Linode, LLC AS63949 Linode, LLC 无
2015/04/28 2015/04/30 45.33.33.228 美国/加利福... AS63949 Linode, LLC 无
2015/04/28 2015/04/29 45.33.48.226 美国/加利福... AS63949 Linode, LLC 无
2015/04/29 2015/04/29 45.33.48.226 52.68.131.221 美国/加利福... 日本/东京都 AS63949 Linode, LLC AS16509 Amazon.com, Inc. XCODEGHOST
2015/04/28 2015/04/28 104.200.26.72 45.33.48.226 美国/加利福... 美国/加利福... AS63949 Linode, LLC AS63949 Linode, LLC 无
2015/04/28 2015/04/28 104.200.26.72 美国/加利福... AS63949 Linode, LLC 无
2015/04/28 2015/04/28 104.200.26.72 45.33.33.228 美国/加利福... 美国/加利福... AS63949 Linode, LLC AS63949 Linode, LLC 无
2015/03/14 2015/04/27 104.238.125.92 美国/亚利桑... AS26496 GoDaddy.com, LLC XCODEGHOST
2015/04/27 2015/04/27 52.68.131.221 52.68.169.28 日本/东京都 日本/东京都 AS16509 Amazon.com, Inc. AS16509 Amazon.com, Inc. 无
历史解析 - 其它记录
最早时间
最近时间
解析结果
类型

人与经验知识积累


360vulcan

360 ALPHA

360烽火实验室

360追日团队

360冰刃实验室

360UNICORNTEAM

360 Gear Team


KEE
TEAM

NIRVAN

360 ADLAB

Marvel Team

SKY-GO
360 VEHICLE CYBER SECURITY

360网络安全响应中心

VULPECKER
TEAM

MeshFire

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）