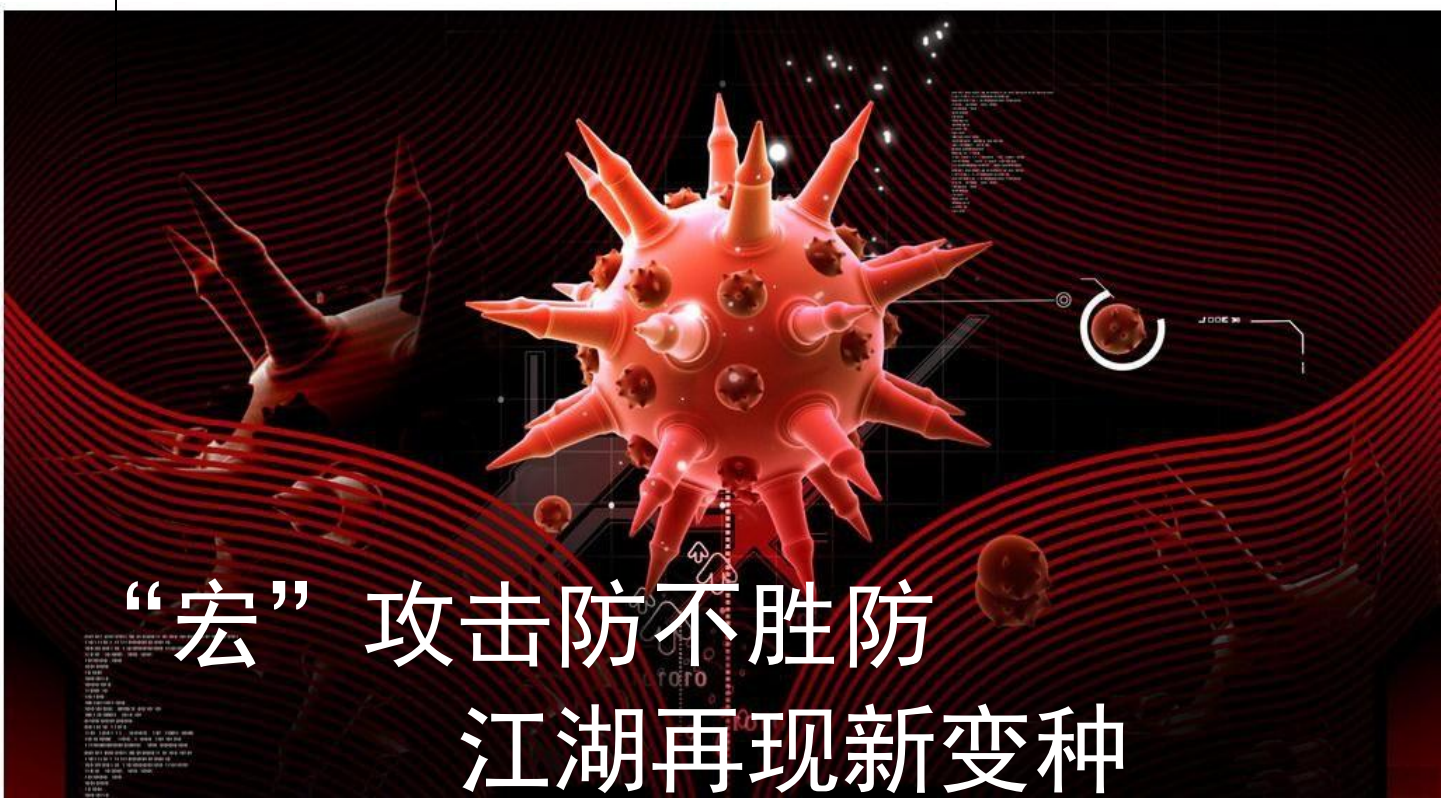
2016 年 11 月



“宏”攻击防不胜防
江湖再现新变种

网络威胁　　全面检测

目录

插图索引

一. “宏”攻击防不胜防，江湖再现新变种

继 2016 年 11 月 4 日发布了《小心，“宏”成为新攻击手法的主力军》报告之后，VenusEye 安全团队又发现一类“宏”攻击恶意样本。

经过分析发现，该类恶意样本与早前披露的样本存在两点不同，可再次**躲避防病毒软件的查杀**。

- **恶意代码隐藏位置不同：**新样本从 TabStrip 控件中获取加密的 shellcode，与早前从 ToggleButton 控件中获取的方式不同。

- **样本调用的特殊函数不同：**新样本调用了 EnumCalendarInfo 函数，该函数主要功能是，遍历日历信息。该函数与早前披露的 EnumDateFormats 的参数相似，调用方法同源。

基于以上两点，我们判断黑客应该还掌握着绕过防病毒软件的“秘密武器”，并且，随时可能发起新的攻击。由于信息安全意义上的 0-Day 是指在安全补丁发布前而被了解和掌握的漏洞信息，基于谨慎原则，我们判定该恶意样本属于“**未知病毒**”。

根据我们的监测，截止到 2016 年 11 月 08 日 15：00PM 为止，这类宏恶意样本可以绕过**绝大多数国内外**流行的防病毒软件的检测。我们将技术细节信息公布，**属于国内首次披露的专项报告**。

我们再次提请广大用户引起注意，该类宏攻击可能爆发，对我国金融、能源、政府、电力等数个敏感行业用户造成威胁。

二. 样本概述和特点

样本名： sample.doc
MD5： 0d1dbb318ca? ? ? ? 8a96e3e9abb307f3616cd

2.1 0x01. 宏代码分析

1、宏恶意代码如下所示：

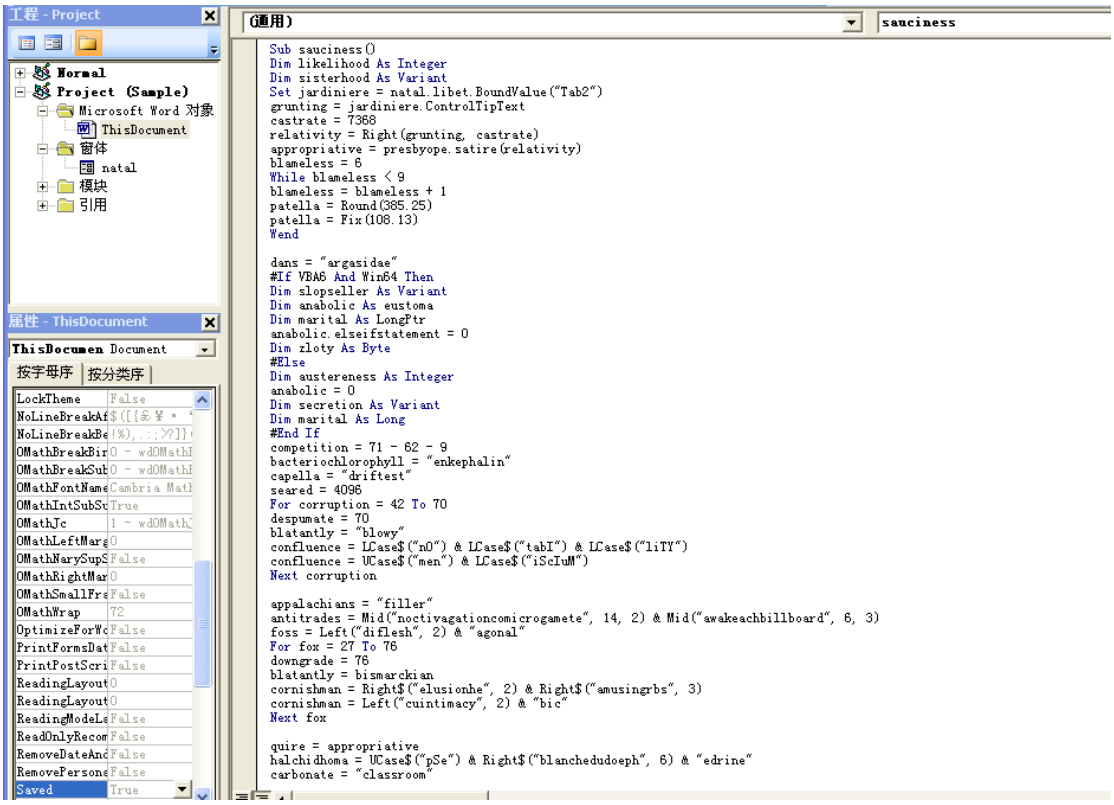


图 2.1 相关宏代码

2、宏代码首先会从一个名为“natal”的窗体的 TabStrip 控件中的 ControlTipText 获取数据。并从右侧取得 7368 个字符。与《20161031_小心，“宏”成为新攻击手法的主力军》之前披露信息不同的是，不从 ToggleButton 控件中获得的数据。

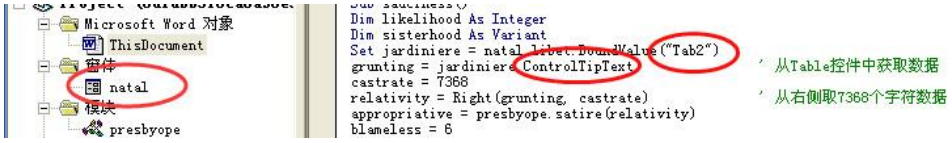


图 2.2　从控件中取数据

3、查看 natal 窗体。初始状态窗体中的 TabStrip 控件仍然是被隐藏起来的。

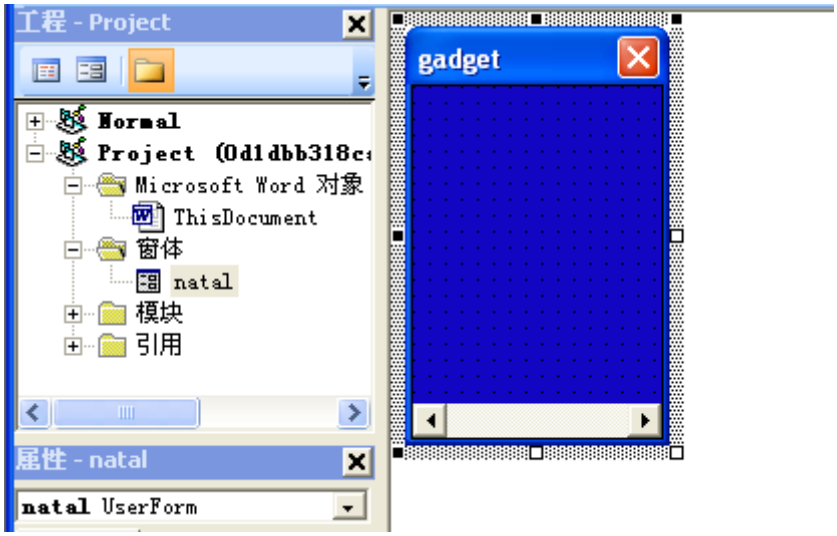


图 2.3　初始状态，TabStrip 控件被隐藏

4、通过拉伸，我们看到隐藏在窗体中的 TabStrip 控件。在 TabStrip 控件的 ControlTipText 属性(ControlTipText 属性可以指定当鼠标悬停在控件上时，显示出来的帮助信息文字）中可以看到保存的数据。

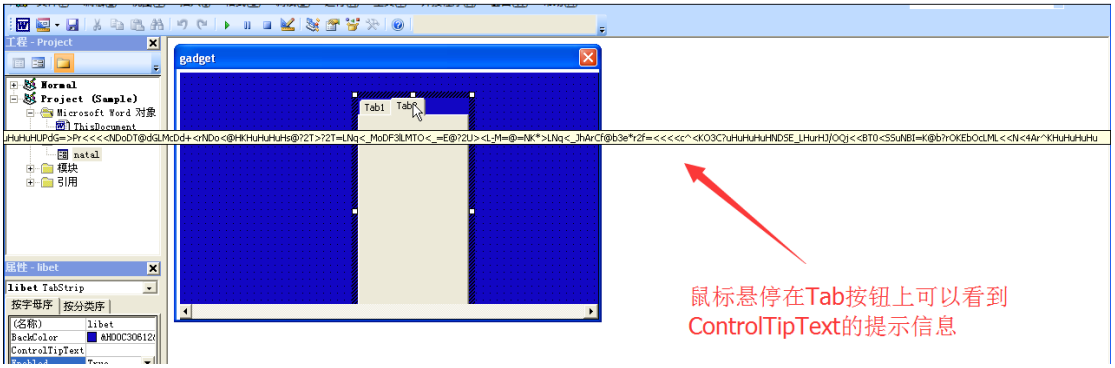


图 2.4　TabStrip 控件的 ControlTipText 属性显示的文字

5、获得 ControlTipText 中的数据后，宏对这段数据进行解密。解密之后，我们看到的依然是一段可执行的 shellcode 代码。Shellcode 与之前相比，属于同源。

图 2.5　新旧 shellcode 对比

6、获得 RtlMoveMemory 和 VirtualAllocEx 等函数地址，并分别保存到相应的变量（bilaterally、madid）中。

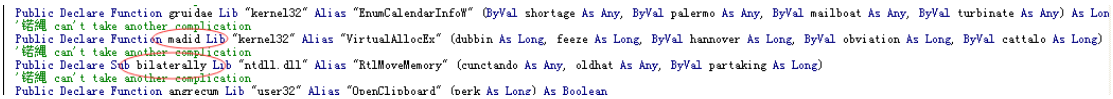


图 2.6　函数地址和相应变量

7、在 buddhism 变量中保存解密出来的 shellcode，调用 VirtuallocEx 分配一段可读可写可执行的内存空间，然后调用 RtlMoveMemory 将 shellcode 拷贝到新分配出来的内存中。

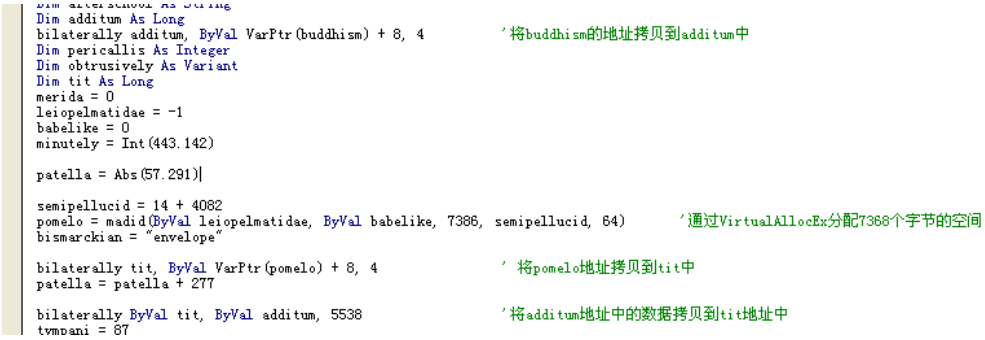


图 2.7　调用 RtlMoveMemory 拷贝 shellcode

8、与之前不同的是，最后其调用的特殊 API 函数有所变化。此次是 EnumCalendarInfoW 函数。可以看到 EnumCalendarInfoW 函数和 EnumDatesFormatW 函数有着类似的参数。第一个参数都可以传入一个回调函数。

```
Public Declare Function deglutition Lib "user32" Alias "EndPaint" (fork As Long, dracunculus As Long) As Long
'铭鸿 can't take another complication
Public Declare Function gruidae Lib "kernel32" Alias "EnumCalendarInfoW" (ByVal shortage As Any, ByVal palermo As Any, ByVal mailboat As Any, ByVal turbinate As Any) As Lon
'铭鸿 can't take another complication
```

图 2.8　宏调用 EnumCalendarInfoW 函数的声明

```
C++

BOOL EnumCalendarInfo(
  _In_ CALINFO_ENUMPROC pCalInfoEnumProc,
  _In_ LCID             Locale,
  _In_ CALID            Calendar,
  _In_ CALTYPE          CalType
);
```

图 2.9　EnumCalendarInfo 函数定义

```
chyme = marital + refuse
Dim ascomycetes As Long
ascomycetes = 124 - 5 - 118
dispersed = gruidae(chyme, minefield, ascomycetes, ascomycetes)      '调用EnumCalendarInfoW函数
whining = 12
```

图 2.10　调用 EnumCalendarInfoW 函数，并将 shellcode 当作回调函数传入

9、使用调试器附加进程，能看到在 EnumCalendarInfoW 函数中进入了相应的 shellcode 代码。

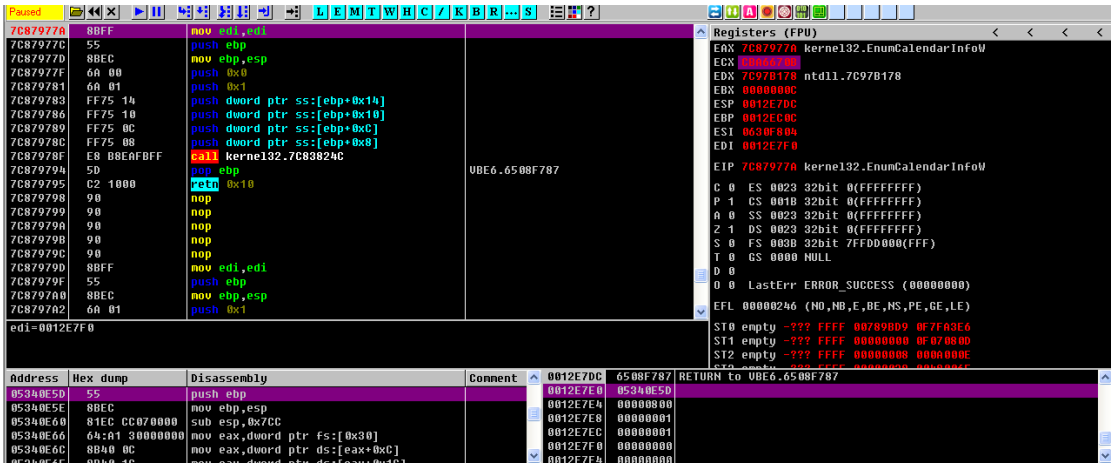


图 2.11　EnumCalendarInfoW 函数入口处代码

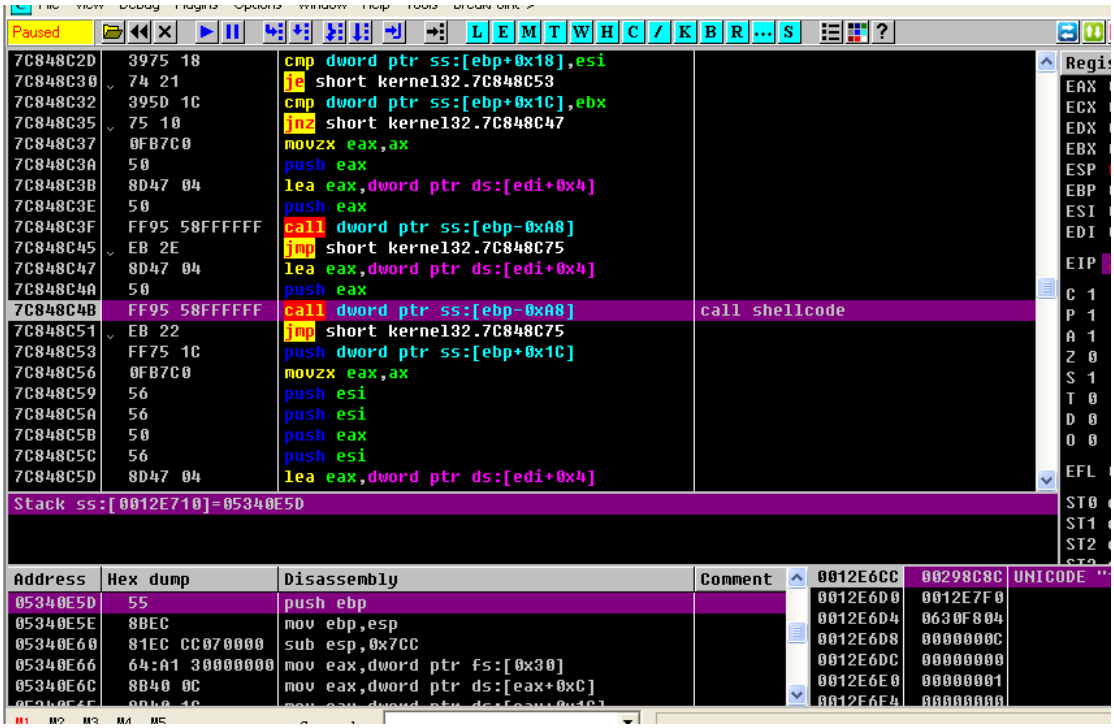


图 2.12　EnumCalendarInfoW 函数调用 shellcode

2.2 0x02. Shellcode 分析

Shellcode 与之前样本基本一致，只是在搜索内嵌 PE 时使用的魔数有所不同。

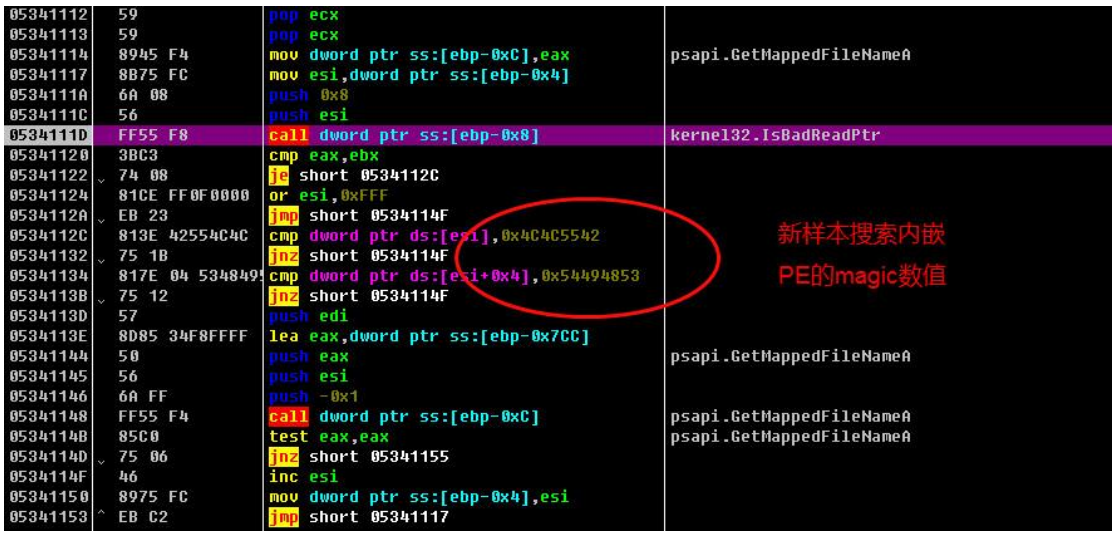
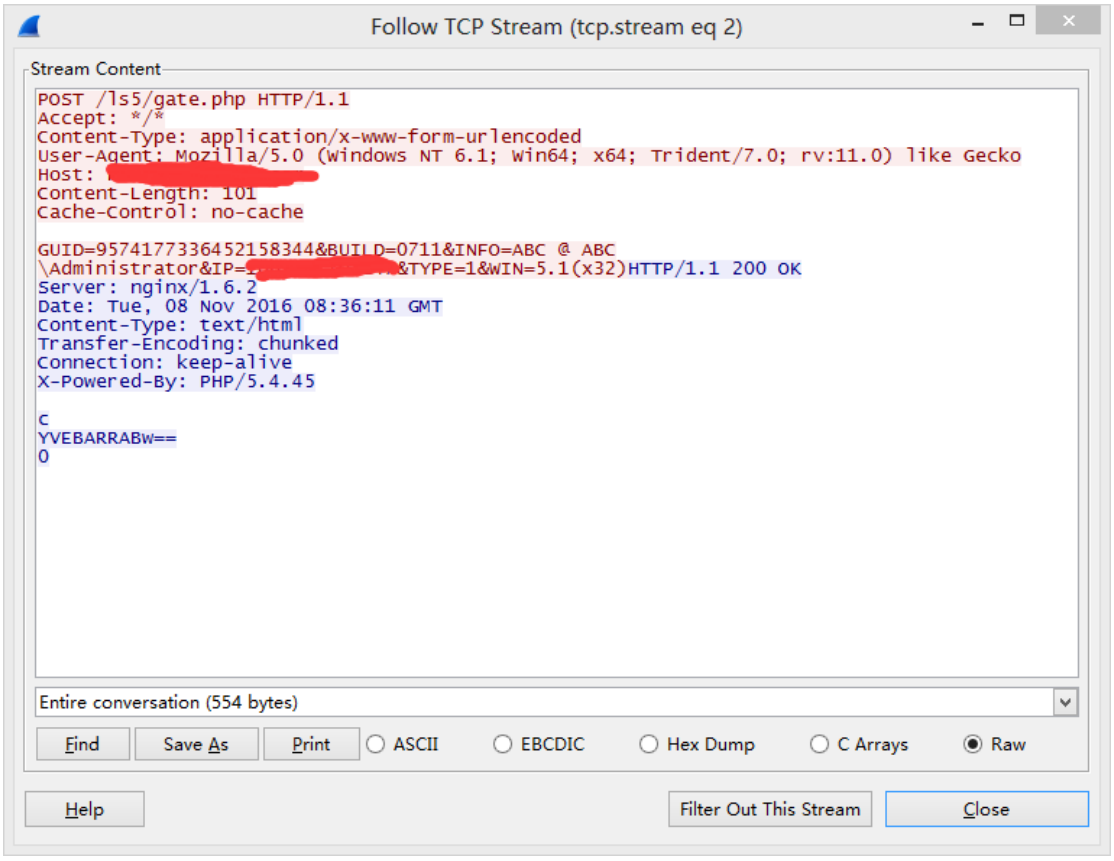


图 2.13　Shellcode 对比数据

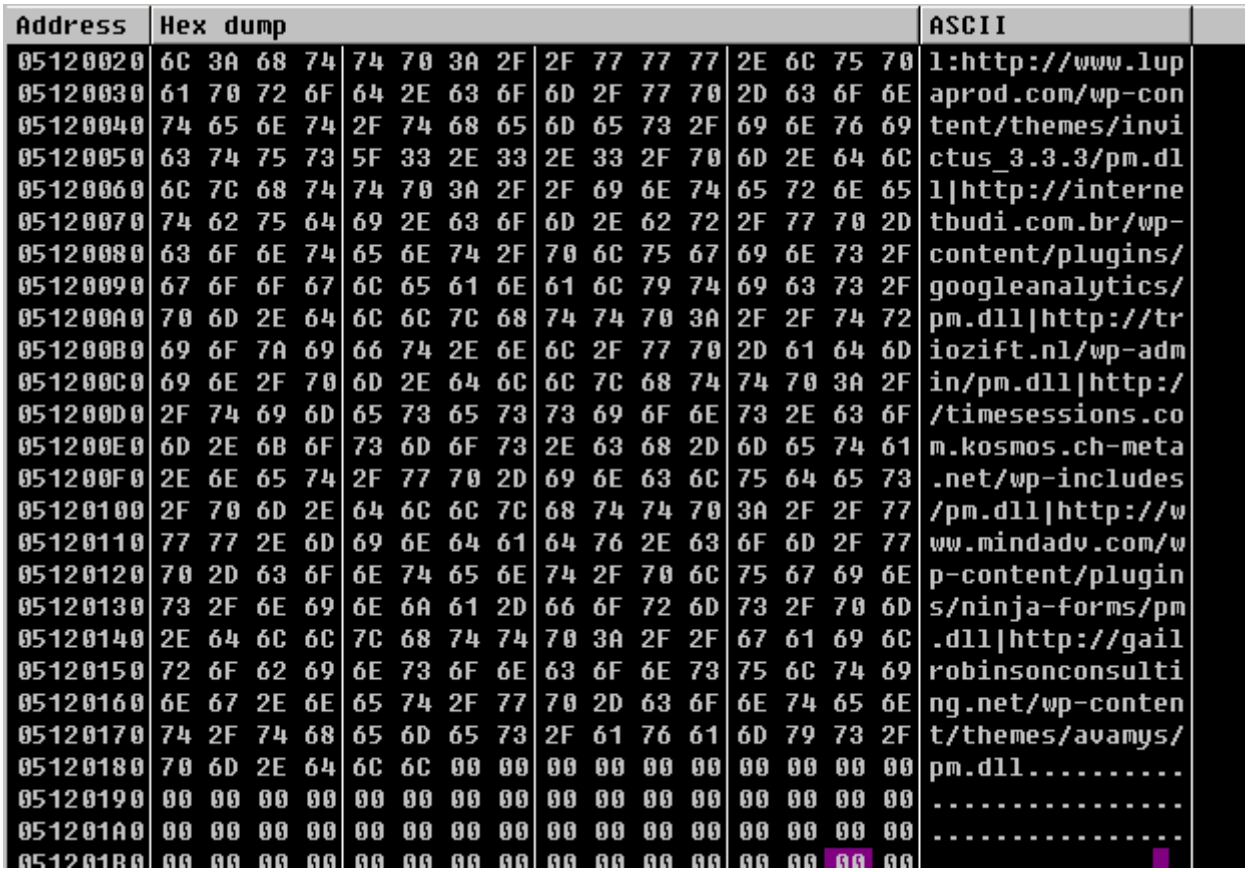
2.3　0x03. PE dump 分析

1、我们将注入到 explorer.exe 中的 PE 文件 dump 出来分析，发现其仍是一个 Hancitor 家族的木马下载器。

2、值得注意的是，木马下载器所链接的恶意 C&C 网站与早前报告披露信息一致。我们在之前分析过旧样本的虚拟机中运行新样本时，服务器不再返回数据。也就是说服务器会记录感染的机器 GUID，感染一次后，便不再重复感染。



3、返回数据解密后，我们看到了一些和早前不同的新的大马下载地址。



Address	Hex dump																ASCII
05120020	6C	3A	68	74	74	70	3A	2F	2F	77	77	77	2E	6C	75	70	l:http://www.lup
05120030	61	70	72	6F	64	2E	63	6F	6D	2F	77	70	2D	63	6F	6E	aprod.com/wp-con
05120040	74	65	6E	74	2F	74	68	65	6D	65	73	2F	69	6E	76	69	tent/themes/invi
05120050	63	74	75	73	5F	33	2E	33	2E	33	2F	70	6D	2E	64	6C	ctus_3.3.3/pm.dl
05120060	6C	7C	68	74	74	70	3A	2F	2F	69	6E	74	65	72	6E	65	l|http://interne
05120070	74	62	75	64	69	2E	63	6F	6D	2E	62	72	2F	77	70	2D	tbudi.com.br/wp-
05120080	63	6F	6E	74	65	6E	74	2F	70	6C	75	67	69	6E	73	2F	content/plugins/
05120090	67	6F	6F	67	6C	65	61	6E	61	6C	79	74	69	63	73	2F	googleanalytics/
051200A0	70	6D	2E	64	6C	6C	7C	68	74	74	70	3A	2F	2F	74	72	pm.dll|http://tr
051200B0	69	6F	7A	69	66	74	2E	6E	6C	2F	77	70	2D	61	64	6D	iozift.nl/wp-adm
051200C0	69	6E	2F	70	6D	2E	64	6C	6C	7C	68	74	74	70	3A	2F	in/pm.dll|http:/
051200D0	2F	74	69	6D	65	73	65	73	73	69	6F	6E	73	2E	63	6F	/timesessions.co
051200E0	6D	2E	6B	6F	73	6D	6F	73	2E	63	68	2D	6D	65	74	61	m.kosmos.ch-meta
051200F0	2E	6E	65	74	2F	77	70	2D	69	6E	63	6C	75	64	65	73	.net/wp-includes
05120100	2F	70	6D	2E	64	6C	6C	7C	68	74	74	70	3A	2F	2F	77	/pm.dll|http://w
05120110	77	77	2E	6D	69	6E	64	61	64	76	2E	63	6F	6D	2F	77	ww.mindadv.com/w
05120120	70	2D	63	6F	6E	74	65	6E	74	2F	70	6C	75	67	69	6E	p-content/plugin
05120130	73	2F	6E	69	6E	6A	61	2D	66	6F	72	6D	73	2F	70	6D	s/ninja-forms/pm
05120140	2E	64	6C	6C	7C	68	74	74	70	3A	2F	2F	67	61	69	6C	.dll|http://gail
05120150	72	6F	62	69	6E	73	6F	6E	63	6F	6E	73	75	6C	74	69	robinsonconsulti
05120160	6E	67	2E	6E	65	74	2F	77	70	2D	63	6F	6E	74	65	6E	ng.net/wp-conten
05120170	74	2F	74	68	65	6D	65	73	2F	61	76	61	6D	79	73	2F	t/themes/avamys/
05120180	70	6D	2E	64	6C	6C	00	00	00	00	00	00	00	00	00	00	pm.dll..........
05120190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
051201A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
051201B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....

图 2.14　C&C 返回的控制指令

三. 样本报告

启明星辰 APT 检测产品可以有效检测该样本

图 3.1 恶意样本调用函数截图

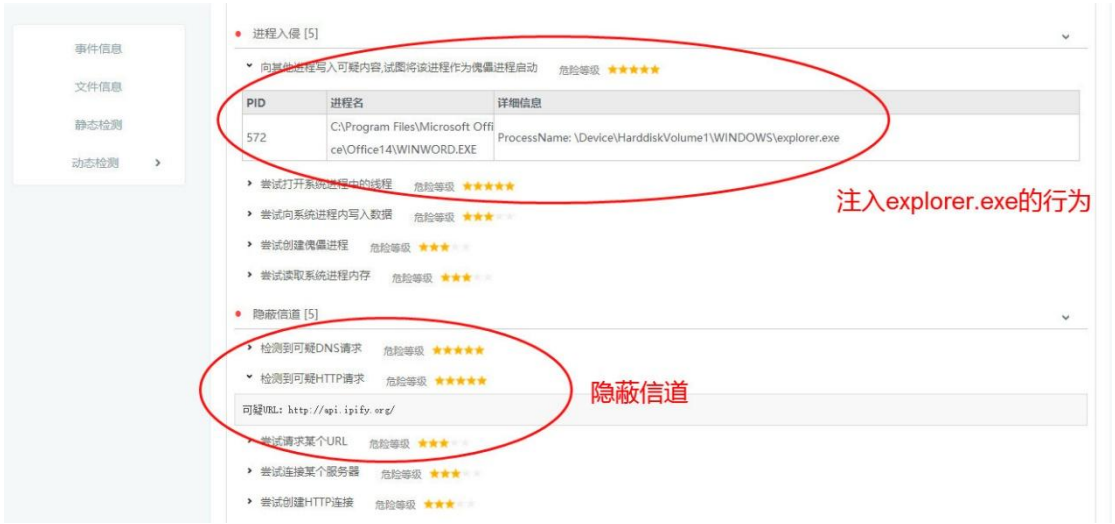


图 3.2 恶意样本注入进程截图

四. 为什么需要部署启明星辰 APT 检测产品

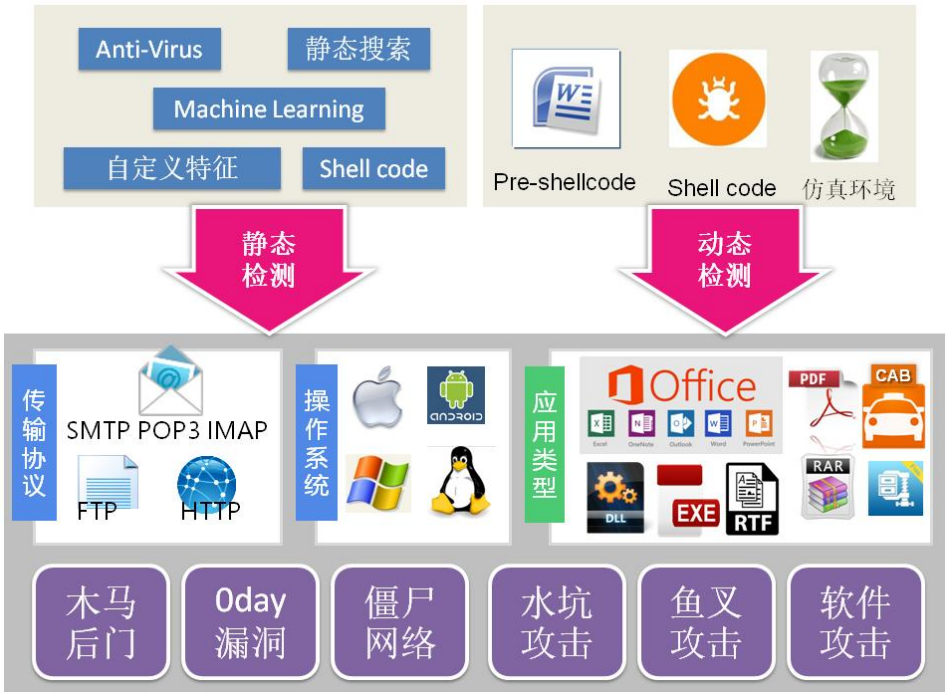
APT 攻击之所以称之为高级持续威胁，是因为攻击本身复杂多维度，手段变化多样，隐藏技术运用多，这让传统的网络安全设备诸如防火墙、入侵检测、入侵防御、防病毒网关、上网行为管理等网关型安全设备难以招架，因此，基于环境模拟的检测技术手段可以填补威胁的不可定义的技术空白，使未知恶意代码和嵌套式攻击、隐秘通道等新形势下的攻击形态无处遁形。

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。

4.1 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：



4.2 关于 VenusEye 安全团队

VenusEye 安全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 安全团队成立至今，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》等十多份专业安全分析报告，欢迎下载查阅。