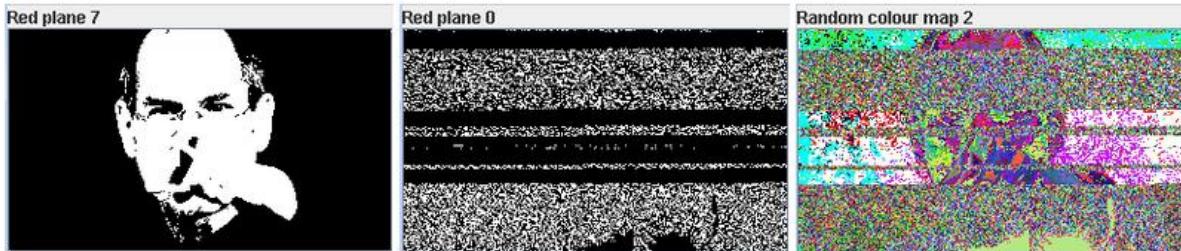


(<http://blog.nsfocus.net/>)

APT技术观察——APT与隐写术

◎ 13 days ago (<http://blog.nsfocus.net/apt-technology-observation-apt-and-steganography/>) ● 伏影实验室 (<http://blog.nsfocus.net/author/fuying-lab/>)



阅读: 207

近期披露的APT组织攻击活动中，我们发现部分组织频繁使用一项历史悠久的信息隐藏技术——隐写术。这些隐写术的实现或复杂或简单，但都有效地增加了攻击的隐匿性与强度。

文章目录



- 前言
- 关于隐写术
- APT组织使用的隐写术
 - 海莲花（OceanLutus）与图像隐写
 - Dukes（APT29）与图像隐写
 - ScarCruft（APT37）与图像隐写
 - 白金（Platinum）与文本隐写
- 参考链接
- 关于伏影实验室
- 关于绿盟威胁情报中心

前言

作为有高度攻击能力的团伙代表，APT组织有时会使用一些非常规的攻击技术。近期披露的APT组织攻击活动中，我们发现部分组织频繁使用一项历史悠久的信息隐藏技术——隐写术。这些隐写术的实现或复杂或简单，但都有效地增加了攻击的隐匿性与强度。

关于隐写术

隐写术（Steganography）一词来源于特里特米乌斯的一本讲述密码学与隐写术的著作Steganographia，该书书名源于希腊语，意为“隐秘书写”。

计算机领域涉及的隐写术载体十分广泛，文本信息、图像信息、音频和视频信息都可以成为隐藏信息的载体，我们只需要将需隐藏的信息拆散并用固定的格式覆盖至信息载体中，就可以实现在欺骗人类感官的同时传递信息。这些隐写术配合一定复杂度的加密技术，即可在相当程度上保证端到端信息传递的隐蔽性，因此该技术经常出现在灰色、黑色领域以及网络攻防对抗当中。

APT组织使用的隐写术

海莲花（OceanLutus）与图像隐写

我们先来看一下大名鼎鼎的海莲花组织在2018年10月的一次攻击中使用的隐写术技术。

该次攻击的原始载荷是一个名为mcvsocfg.dll的动态链接库文件，该文件模仿McAfee旗下同名文件的导出表，使用自利用的方式将自身加载运行。当受害者打开同目录下的安全程序mcdos.exe时，该dll中的恶意代码被调用执行。



DLL文件包含以下导出表：

Name	Address	Ordinal
Cleanup	10077FO0	1
DllRegisterServer	10077EA0	2
DllUnregisterServer	10077E40	3
McVsoCfgGetObject	10077DE0	4
MigrateVirusScanSettings	10077D80	5
ServiceCrtMain	10077CC0	6
SyncVirusScanSettings	10077D20	7
ValidateDrop	10077C60	8
DllEntryPoint	10059282	[main entry]

导出表中所有函数都执行同样的恶意代码，读取system.ini文件并以此解密隐写术图像中的信息：

```
int Cleanup()
{
    HANDLE v0; // ebx
    void *v1; // edi
    void *v2; // esi
    SIZE_T dwSize; // [esp+Ch] [ebp-4h]

    rbsystemini_10002480();
    v0 = GetCurrentProcess();
    v1 = (void *)decode_steganography_image_100022D0((int *)&dwSize);
    v2 = VirtualAllocEx(v0, 0, dwSize, 0x1000u, 0x40u);
    WriteProcessMemory(v0, v2, v1, dwSize, 0);
    Free(v1);
    return ((int (*)(void))v2)();
}
```

隐写术图像在dll同目录下，名为x5j3trra.png：



x5j3trra.png

阅读关键代码可发现，该程序将png图像每个像素RGB值的低位拼合成一个字节，再将所有字节组合为加密字节串：

```
++v15;
v16 = v23;
*(BYTE *) (v13++ + v25) = BYTE2(dwARGB) & 7 | 8 * (8 * dwARGB | BYTE1(dwARGB) & 7);
v14 = v26;
```

此处dwARGB值在内存中遵循BGRA的字节排列，因此每个像素的隐藏信息提取过程如下（以图片头部像素0xFF4586E2为例）：

通道	BLUE	GREEN	RED	ALPHA
位	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
值	0 1 0 0 0 1 1 1	0 1 1 0 0 0 0 1	1 1 0 1 0 0 0 1 0	1 1 1 1 1 1 1 1 1
取位	0 1	0 1 1	1 0 1	
位	0 1 2 3 4 5 6 7			
结果	1 0 1 0 1 1 0 1			

以上提取结果为0xB5，即图像的此像素中隐藏了值为0xB5的单字节信息。

通过以上方式，程序将隐藏在png图像中的加密字节串提取出来，之后使用AES-CBC和异或解密出最终载荷：

```
if ( result )
{
    key = 0;
    iv = 0;
    init_key_iv_10002880(&key, &iv);
    pdecryptedbytes = aes_decode_100028B0(
        (int)pencryptedbytes,
        (int)encryptedbyteslen,
        key,
        iv,
        (size_t *)&decryptedbyteslen);
    free(pencryptedbytes);
    v5 = 0;
    if ( decryptedbyteslen )
    {
        do
            pdecryptedbytes[v5++] ^= v1;
        while ( v5 < decryptedbyteslen );
    }
    sub_10001AB0((int)&v6, &unk_1007B3BE);
    sub_10002650(v6, v7, v8, v9, v10, v11);
    result = pdecryptedbytes;
    *a1 = decryptedbyteslen;
}
```

该最终载荷为多层shellcode加载器形式的DenesRAT木马，详细分析可参见由伏影实验室发布的《海莲花（APT32）组织 DenesRAT木马与相关攻击链分析》。

在这次攻击中，海莲花组织使用了最常见的隐写术手法——图片像素低位隐写，这样的手段生成的图像足以欺骗人类的视觉；再通过有一定难度的加密方式，使得安全人员即使获取到了包含隐写信息的图像也无法还原出攻击载荷，大大增加了攻击流程的隐匿性。

Dukes (APT29) 与图像隐写

同样的手段出现在APT组织Dukes的攻击流程中。在最近由ESET披露的攻击活动中，Dukes使用的攻击载荷PolyglotDuke与RegDuke在C&C通信阶段使用了图像隐写术作为隐匿手段。这些载荷使用的隐写方式与上文所述海莲花隐写术基本相同，在png图像每个像素RGB值的低位中存放了1字节的信息，且完整信息同样是使用AES加密的密文，唯一不同点在于取用的RGB像素位与最终拼接顺序。该隐写方式取用的RGB通道位置、位数及组合方式示例如下：

通道	BLUE							GREEN							RED							ALPHA											
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
值	1	0	0	0	1	1	1	0	0	1	0	0	1	1	1	1	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	
取位	1	0	0						0	1	0						0	1															
位	0	1	2	3	4	5	6	7																									
结果	1	0	0	0	1	0	0	1																									

同时，ESET的报告中展示了以下隐写图像：




```

if ( vposSELFSIGN < vdwNumberOfBytesRead )
{
    if ( v20 >= 0x20 )
    {
        do
        {
            *(_m128i *)((char *)vreadbuffer + i) = _mm_xor_si128(
                *(_m128i *)((char *)vreadbuffer + i),
                (_m128i)xmmword_1001EC00);
            *(_m128i *)((char *)vreadbuffer + i + 16) = _mm_xor_si128(
                (_m128i)xmmword_1001EC00,
                *(_m128i *)((char *)vreadbuffer + i + 16));
            i += 32;
        }
        while ( i < vdwNumberOfBytesRead - (v20 & 0x1F) );
    }
    for ( ; i < vdwNumberOfBytesRead; ++i )
        *((BYTE *)vreadbuffer + i) ^= 0x49u;
}

```

解密后的攻击载荷为ROKRAT后门，其主要功能为窃取用户主机信息并上传至指定云服务中（Box, Dropbox, Pcloud, Yandex）。该后门会被植入到winlogon.exe进程中。

该次攻击事件中，ScarCrft组织使用了图片隐写更直接的手法，即直接将加密数据植入图像数据末尾。该手法优点在于可以在同等大小的图像中塞入更多隐藏信息，而缺点在于数据整体暴露在合法文件结构以外，容易被静态检测手段检测。

白金（Platinum）与文本隐写

卡巴斯基在今年5月的报告中提到，APT组织Platinum也在使用隐写术传递载荷。

与海莲花和ScarCrft不同，Platinum使用了文本隐写术。卡巴斯基报告中提到了两种文本隐写术手法：关键词隐写和空白隐写。这两种文本隐写方式的思路截然相反，关键词隐写将内容隐藏在可见字符中，空白隐写则将之隐藏至不可见部分。

报告中提到的关键词隐写部分如下：

```

25     <!--1234567890--<body>
26         <table align="center" bgcolor="white" border="0" cellpadding="4" rules="no
27             <tr align="center" bgcolor="white" valign="middle">
28                 <td bgcolor="white" align="center" colspan="1" rowspan="1"></td>
29                 <td align="center" bgcolor="white" colspan="1" rowspan="1"></td>
30                 <td align="center" bgcolor="white" colspan="1" rowspan="1"></td>
31                 <td align="center" bgcolor="white" colspan="1" rowspan="1"></td>|<br/>
32                 <td align="center" colspan="1" rowspan="1" style="background-color: white;"></td>
33                 <td align="center" colspan="1" rowspan="1" style="background-color: white;"></td>
34                 <td align="center" colspan="1" rowspan="1" style="background-color: white;"></td>
35                 <td align="center" colspan="1" rowspan="1" style="background-color: white;"></td>
36                 <td align="center" colspan="1" rowspan="1" style="background-color: white;"></td>
37                 <td align="center" colspan="1" rowspan="1" style="background-color: white;"></td>
38             </tr>
39         </table>
40         <table cellspacing="0" width="100" bgcolor="white" frame="void" align="cen

```

该html文件的28行到37行语句中包含四个属性：bgcolor、align、colspan、rowspan。由于html对属性的顺序不敏感，这些属性的位置可以随意调换，Platinum正是利用了这一点来传递信息。简单计算可知，这四个属性组成的四进制数据有24种不同的排列，可指代0至0x17的十六进制数据，因此一行携带的隐藏信息量超过了4bit。

空白隐写则如下所示：

```

943     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
944     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
945     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
946     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
947     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
948     --1234567890--></body>
949     </html>

```

位于文件943~947行的隐写内容由空格键（0x20）和制表键（0x9）组成，因此对阅读者不可见。由关键词隐写我们可以联想到，该部分的隐写内容是二进制数据，事实也正是如此。然而，由于二进制数据能够装载的信息很有限，常规数据一般需要经过压缩来获得更小的二进制空间。卡巴斯基报告指出，该处的二进制数据是由ICE算法压缩的（<http://www.darkside.com.au/snow/>）。

从Platinum组织使用的隐写术中可以发现，隐写术的本质是将二进制数据转为其他进制数据并放入合适的载体中。因此，隐写术的载体可以是现代计算机网络中任何信息载体形式，攻击者是否使用隐写术更多取决于载体是否易于传播以及转换后信息是否足够隐蔽。

参考链接

https://threatvector.cy lance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html (https://threatvector.cy lance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html)

<https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/> (<https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/>)

<https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/> (<https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/>)

<https://securelist.com/platinum-is-back/91135/> (<https://securelist.com/platinum-is-back/91135/>)

<http://www.darkside.com.au/snow/> (<http://www.darkside.com.au/snow/>)

关于伏影实验室



伏影实验室专注于安全威胁研究与监测技术，包括但不限于威胁识别技术，威胁跟踪技术，威胁捕获技术，威胁主体识别技术。研究目标包括：僵尸网络威胁，DDOS对抗，WEB对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁及新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。

关于绿盟威胁情报中心

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技为落实智慧安全2.0战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

文章分类：威胁通报 (<http://blog.nsfocus.net/category/threatalerts/>)

文章关键词：APT (<http://blog.nsfocus.net/tag/apt/>) , APT32 (<http://blog.nsfocus.net/tag/apt32/>) , NSFOCUS (<http://blog.nsfocus.net/tag/nsfocus/>) , Steganography (<http://blog.nsfocus.net/tag/steganography/>) , 伏影实验室 (<http://blog.nsfocus.net/tag/%e4%bc%8f%e5%bd%b1%e5%ae%9e%e9%aa%8c%e5%ae%a4/>) , 海莲花 (<http://blog.nsfocus.net/tag/%e6%b5%b7%e8%8e%b2%e8%8a%b1/>) , 隐写术 (<http://blog.nsfocus.net/tag/%e9%9a%90%e5%86%99%e6%9c%af/>)

转载请注明：“转自绿盟科技博客”：原文链接 (<http://blog.nsfocus.net/apt-technology-observation-apt-and-steganography/>)。

文章收录：

← 绿盟科技互联网安全威胁周报NSFOCUS-2019-43

【威胁通告】Apache Solr远程命令执行漏洞 → (<http://blog.nsfocus.net/apache-solr2019-10-31/>)

发表评论

要发表评论，您必须先登录 (http://blog.nsfocus.net/wp-login.php?redirect_to=http%3A%2F%2Fblog.nsfocus.net%2Fapt-technology-observation-apt-and-steganography%2F)。

绿盟科技博客精华文章

学习手册：浅析DDoS的攻击及防御 (<http://blog.nsfocus.net/analysis-ddos-attack-defense/>)

学习手册：盘点DDoS带来的误会 (<http://blog.nsfocus.net/inventory-ddos-errors/>)

移动APP安全测试要点 (<http://blog.nsfocus.net/mobile-app-security-security-test/>)

Dedecms远程写文件漏洞分析 (<http://blog.nsfocus.net/dedecms-write-file-vuln/>)

【干货分享】XSS攻击进阶篇——那些年我们看不懂的XSS (<http://blog.nsfocus.net/xss-advance/>)

两步邮件订阅，方便获取文章

欢迎订阅！现在已有6 705个朋友订阅了。
在后续邮件的尾部，您可以退订及修改订阅内容。

选择订阅组：

- 最新文章
- 技术分享
- 漏洞分析
- 运维安全
- Web安全
- 安全报告

邮件 *

[马上订阅！](#)

绿盟科技博客功能

注册 (<http://blog.nsfocus.net/wp-login.php?action=register>)

登录 (<http://blog.nsfocus.net/wp-login.php>)

文章RSS (Really Simple Syndication) (<http://blog.nsfocus.net/feed/>)

评论RSS (Really Simple Syndication) (<http://blog.nsfocus.net/comments/feed/>)

WordPress.org (<https://cn.wordpress.org/>)

绿盟科技博客文章标签

绿盟科技 (<http://blog.nsfocus.net/tag/%e7%bb%bf%e7%9b%9f%e7%a7%91%e6%8a%80/>) 漏洞

(<http://blog.nsfocus.net/tag/%e6%bc%8f%e6%b4%9e/>) 远程代码执行漏洞

(<http://blog.nsfocus.net/tag/%e8%bf%9c%e7%a8%8b%e4%bb%a3%e7%a0%81%e6%89%a7%e8%a1%8c%e6%bc%8f%e6%b4%9e/>) 绿盟科技漏洞库 (<http://blog.nsfocus.net/tag/%e7%bb%bf%e7%9b%9f%e7%a7%91%e6%8a%80%e6%bc%8f%e6%b4%9e%e5%ba%93/>) NSFOCUS

(<http://blog.nsfocus.net/tag/nsfocus/>) EnglishVersion (<http://blog.nsfocus.net/tag/englishversion/>) DDoS (<http://blog.nsfocus.net/tag/ddos/>) 技术博客

(<http://blog.nsfocus.net/tag/%e6%8a%80%e6%9c%af%e5%8d%9a%e5%ae%a2/>) 远程代码执行

(<http://blog.nsfocus.net/tag/%e8%bf%9c%e7%a8%8b%e4%bb%a3%e7%a0%81%e6%89%a7%e8%a1%8c/>) 云安全

(<http://blog.nsfocus.net/tag/%e4%ba%91%e5%ae%89%e5%85%a8/>) 威胁情报

(<http://blog.nsfocus.net/tag/%e5%a8%81%e8%83%81%e6%83%85%e6%8a%a5/>) 网络安全

(<http://blog.nsfocus.net/tag/%e7%bd%91%e7%bb%9c%e5%ae%89%e5%85%a8/>) 威胁 (<http://blog.nsfocus.net/tag/%e5%a8%81%e8%83%81/>) 物联网安全

(<http://blog.nsfocus.net/tag/%e7%89%a9%e8%81%94%e7%bd%91%e5%ae%89%e5%85%a8/>) 高危漏洞

(<http://blog.nsfocus.net/tag/%e9%ab%98%e5%8d%b1%e6%bc%8f%e6%b4%9e/>) 绿盟科技博客

(<http://blog.nsfocus.net/tag/%e7%bb%bf%e7%9b%9f%e7%a7%91%e6%8a%80%e5%8d%9a%e5%ae%a2/>) 威胁通告

(<http://blog.nsfocus.net/tag/%e5%a8%81%e8%83%81%e9%80%9a%e5%91%8a/>) rsa2018 (<http://blog.nsfocus.net/tag/rsa2018/>) 安全会议

(<http://blog.nsfocus.net/tag/%e5%ae%89%e5%85%a8%e4%bc%9a%e8%ae%ae/>) 安全周报

(<http://blog.nsfocus.net/tag/%e5%ae%89%e5%85%a8%e5%91%a8%e6%8a%a5/>) ddos攻击事件

([http://blog.nsfocus.net/tag/ddos%e6%94%bb%e5%87%bb/](http://blog.nsfocus.net/tag/ddos%e6%94%bb%e5%87%bb%e4%ba%8b%e4%bb%b6/)) DDoS攻击

(<http://blog.nsfocus.net/tag/ddos%e6%94%bb%e5%87%bb/>) 云计算 (<http://blog.nsfocus.net/tag/%e4%ba%91%e8%a1%e7%ae%97/>) 大数据

(<http://blog.nsfocus.net/tag/%e5%a4%a7%e6%95%b0%e6%8d%ae/>) 勒索软件

(<http://blog.nsfocus.net/tag/%e5%8b%92%e7%b4%a2%e8%bd%af%e4%bb%b6/>) 安全意识

(<http://blog.nsfocus.net/tag/%e5%ae%89%e5%85%a8%e6%84%8f%e8%af%86/>) 恶意软件

(<http://blog.nsfocus.net/tag/%e6%81%b6%e6%84%8f%e8%bd%af%e4%bb%b6/>) 物联网

(<http://blog.nsfocus.net/tag/%e7%89%a9%e8%81%94%e7%bd%91/>) 漏洞分析

(<http://blog.nsfocus.net/tag/%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90/>) 态势感知

(<http://blog.nsfocus.net/tag/%e6%80%81%e5%8a%bf%e6%84%9f%e7%9f%a5/>)

最新文章

【威胁通告】Squid多个高危漏洞预警通告 (<http://blog.nsfocus.net/cve-2019-12526-cve-2019-18679-cve-2019-18678/>)

【威胁通告】开源压缩库Libarchive代码执行漏洞 (CVE-2019-18408) (<http://blog.nsfocus.net/cve-2019-18408/>)

绿盟科技互联网安全威胁周报NSFOCUS-2019-44 (<http://blog.nsfocus.net/nsfocus-2019-44/>)

网络安全威胁月报NSFOCUS-2019-10 (<http://blog.nsfocus.net/nsfocus-2019-10/>)

Jenkins 路由解析及沙箱绕过漏洞分析报告(上) (<http://blog.nsfocus.net/jenkins-routing-resolution-and-sandbox-bypass-vulnerability-analysis-report/>)



【威胁通告】Apache Solr Velocity远程代码执行漏洞处置手册 (<http://blog.nsfocus.net/ns-2019-0046/>)

【威胁通告】Apache Solr远程命令执行漏洞 (<http://blog.nsfocus.net/apache-solr2019-10-31/>)

APT技术观察——APT与隐写术 (<http://blog.nsfocus.net/apt-technology-observation-apt-and-steganography/>)

绿盟科技互联网安全威胁周报NSFOCUS-2019-43 (<http://blog.nsfocus.net/nsfocus-2019-43/>)

Splinter新APT攻击工具透析 (<http://blog.nsfocus.net/splinters-new-apt-attack-tool-dialysis/>)

友情链接

绿盟科技官网 (<http://www.nsfocus.com.cn>)

绿盟威胁情报中心NTI (<https://nti.nsfocus.com/>)



群名称:绿盟安全爱好者

群号:956543462



