SEGURANÇA
DESCOMPLICADA

Análise de Processos

Follina: Malware 0-Day

Flávio Costa
Especialista em Cibersegurança

Quem Sou Eu?

$WHOAMI System Owner/User Discovery (T1033)

Especialista em cibersegurança, escritor, palestrante e criador de conteúdo.

- Business Development Engineer na Fortinet
- Instrutor oficial e Subject Matter Expert (SME) da CompTIA.
- Professor convidado PUC-PR & Hackers do Bem.

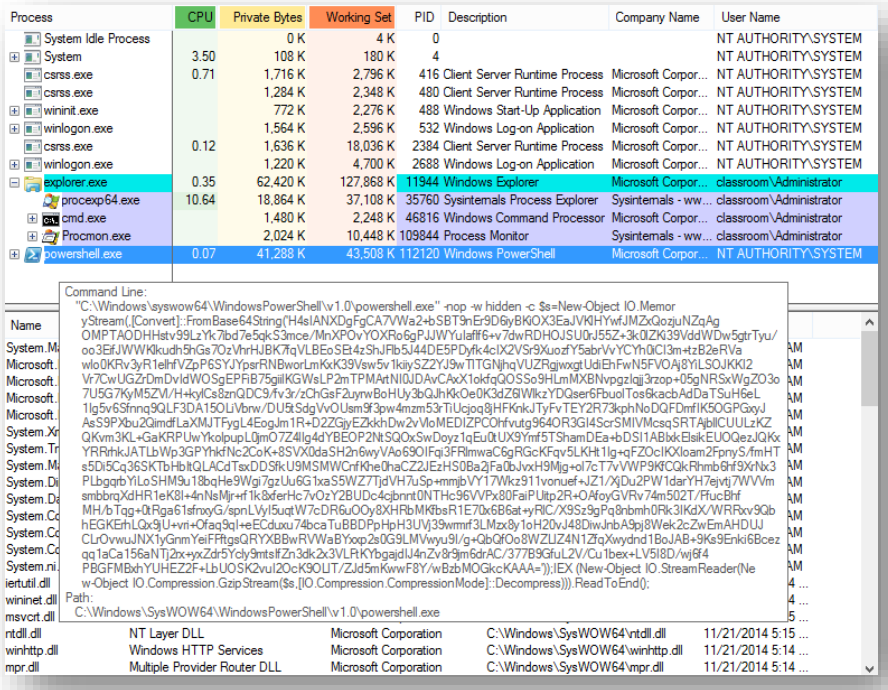
Formado em:

- Gestão de TI
- MBA em Cybersecurity, Ethical Hacking & DevSecOps
- MBA em Arquitetura e Gestão de Infraestrutura de TI
- MBA em Digital Companies & E-business Revolution

Certificações: Meraki CMNA, Cisco CCNP Security e Enterprise, CCDA e CyberOps; (ISC)² CC; EC-Council C|CISO; CompTIA A+, Network+, Cloud+, Security+, PenTest+, CySA+ e CASP+.

@LinkedIn @Instagram @YouTube

Análise de Processos



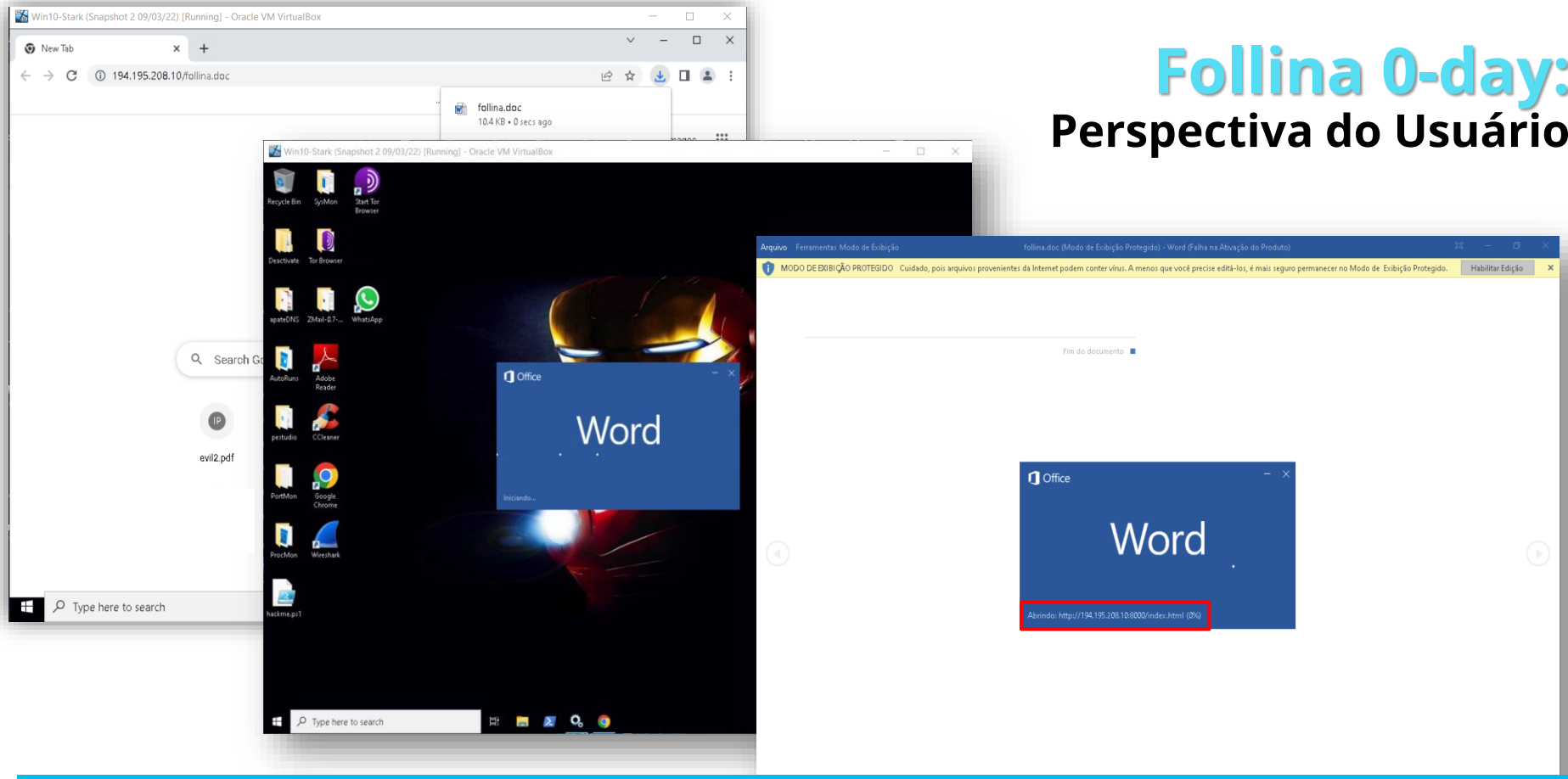
Screenshot: Process Explorer docs.microsoft.com/en-us/sysinternals.

- **Threat hunting** e o **monitoramento de segurança** devem utilizar técnicas baseadas em comportamento para identificar infecções. Isso significa uma análise detalhada dos processos em execução na memória do sistema. Para realizar uma análise de comportamento anormal de processo de forma eficaz, é necessário ter uma noção do que é "normal" em um sistema e identificar desvios (IOCs) em um sistema potencialmente infectado. Além disso, é necessário utilizar ferramentas de análise apropriadas. O Sysinternals (https://docs.microsoft.com/pt-br/sysinternals) é um conjunto de ferramentas projetadas para ajudar na solução de problemas com o Windows, e muitas dessas ferramentas são adequadas para investigar problemas de segurança.

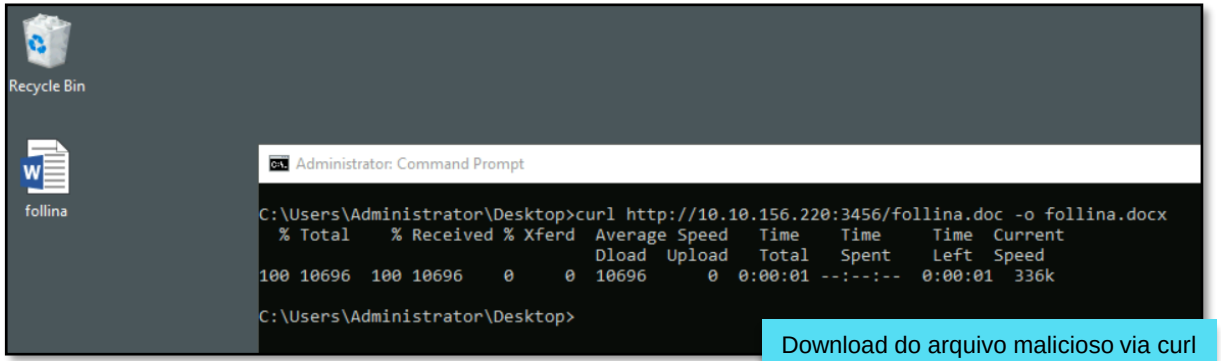
- Juntamente com a observação de como um processo interage com o sistema de arquivos, a atividade de rede é uma das maneiras mais confiáveis de identificar malware. Dados de ameaças podem ser usados para correlacionar conexões a endereços IP e domínios conhecidos como ruins, mas o malware pode tentar se conectar a endpoints em constante mudança, utilizando técnicas como fast-flux e algoritmos de geração de domínio (DGA). Ele também pode tentar usar mídias sociais e serviços em nuvem para se misturar ao tráfego legítimo.

**Fast flux é uma técnica de DNS usada para mascarar botnets, alternando rapidamente entre uma rede de hosts comprometidos, agindo como proxies, permitindo que cibercriminosos atrasem ou evitem a detecção. O fast flux permite que as botnets se escondam por trás de uma rede de hosts comprometidos em rápida mudança, agindo como proxies.*

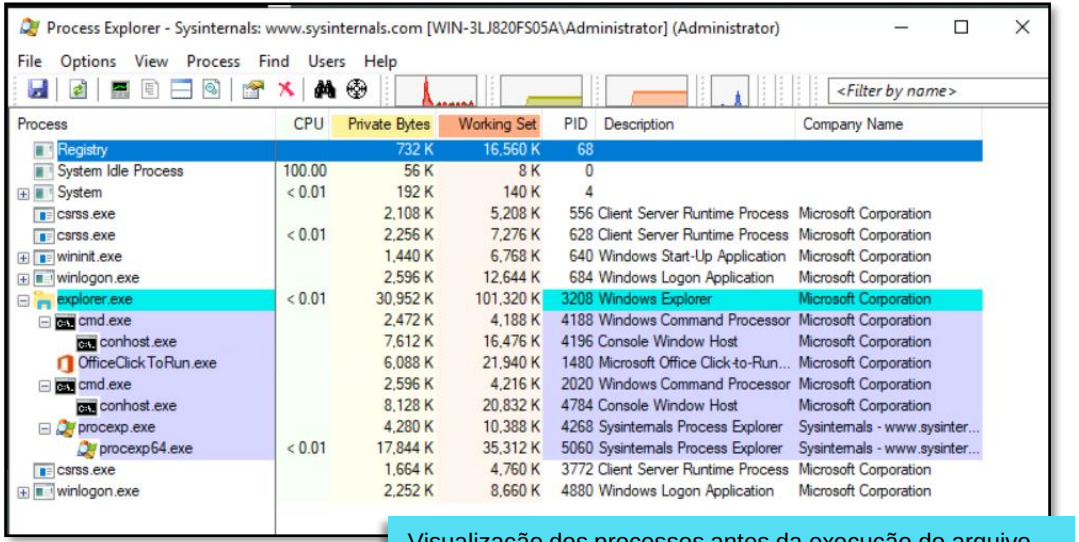
Follina 0-day:
Perspectiva do Usuário



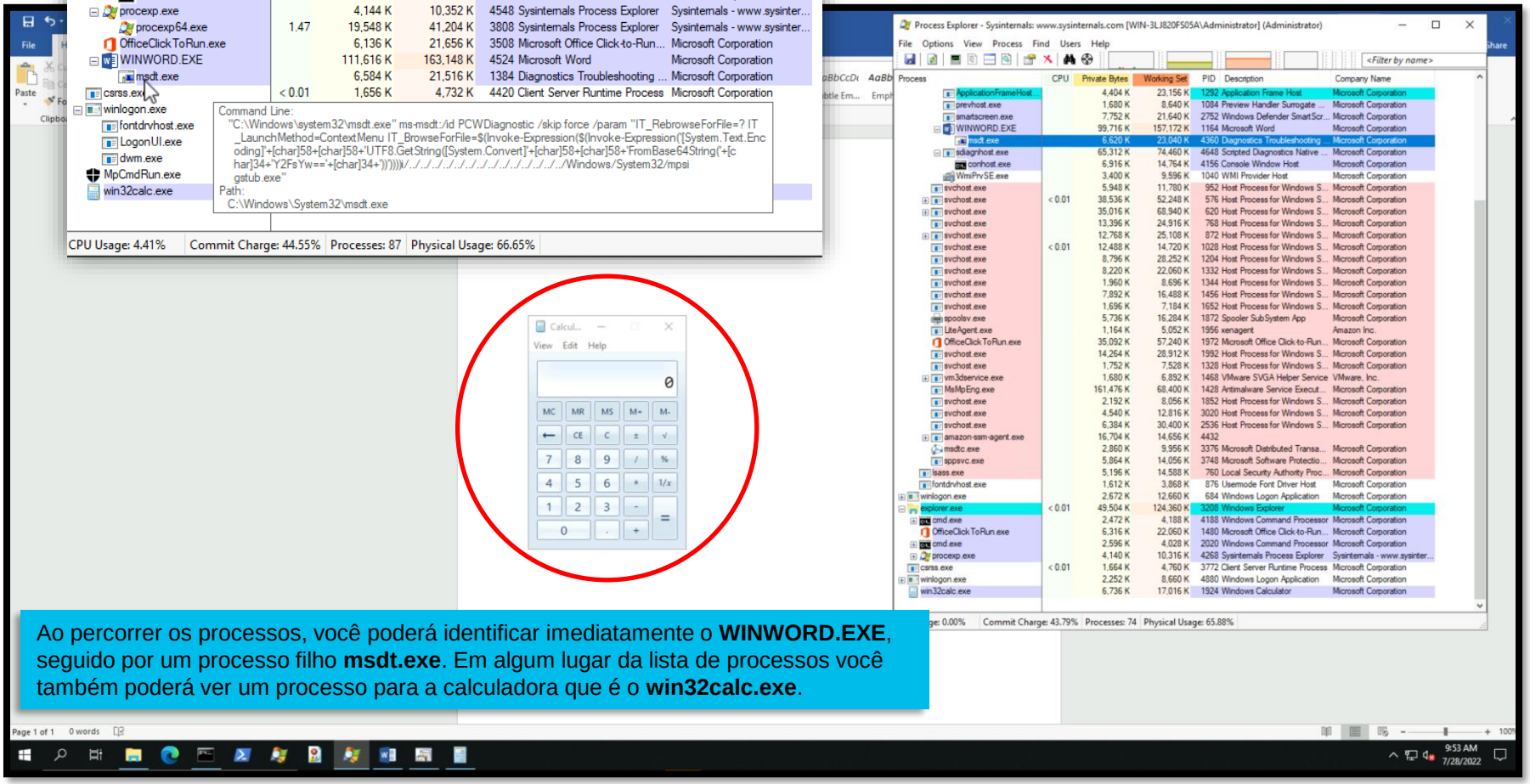
Follina é uma vulnerabilidade zero-day que aproveita os manipuladores de URL integrados da MS para acionar o processo Microsoft Support Diagnostic Tool (Ferramenta de Diagnóstico de Suporte da Microsoft (MSDT), que pode ser usado para executar código na máquina da vítima. Foi nomeada "Follina", em referência à cidade na Itália cujo código de área coincide com os números escritos no arquivo malicioso encontrado no site Virus Total. Em resumo, **o Follina permite que hackers executem código malicioso por meio do recurso de modelo remoto no Microsoft Word.**



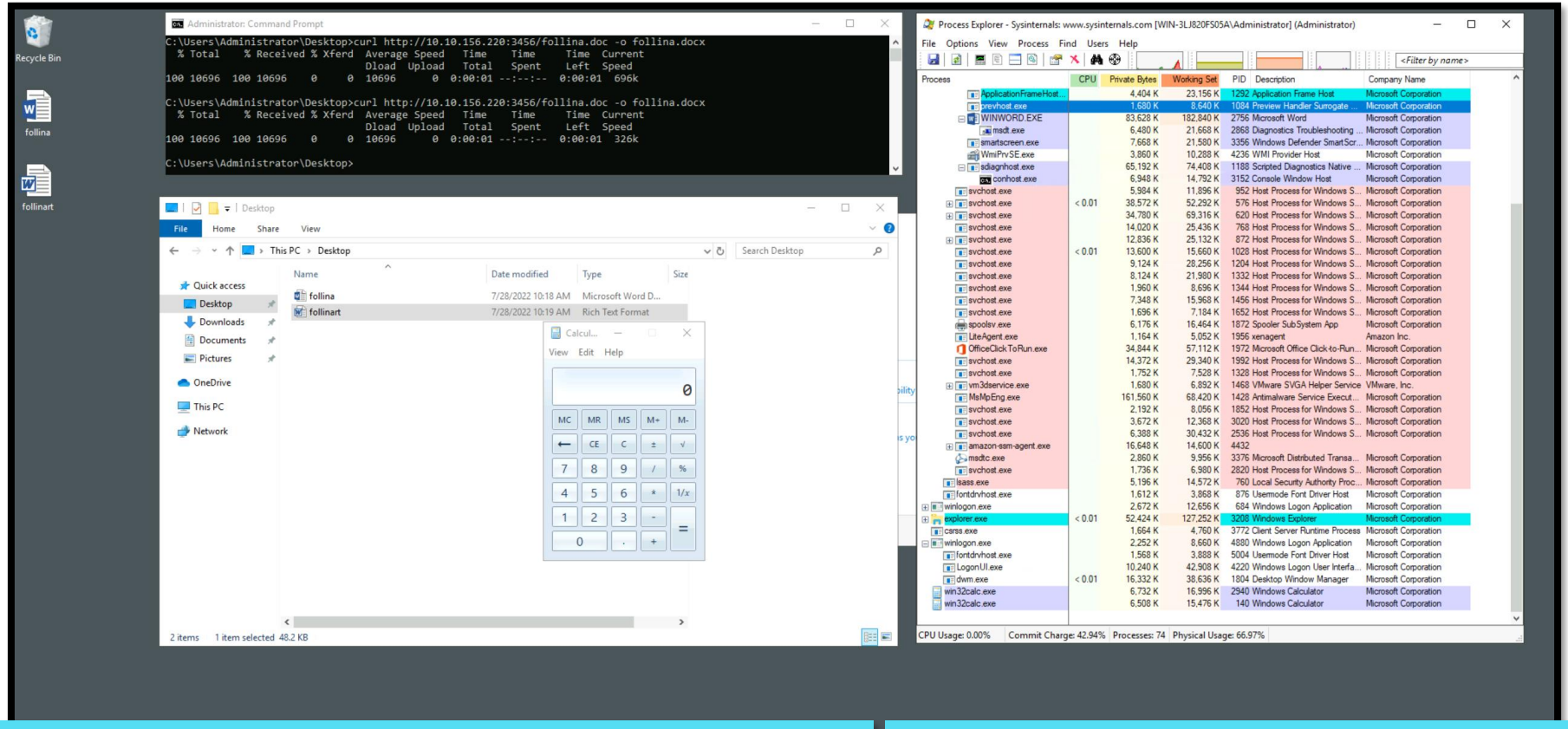
Download do arquivo malicioso via curl



Visualização dos processos antes da execução do arquivo.



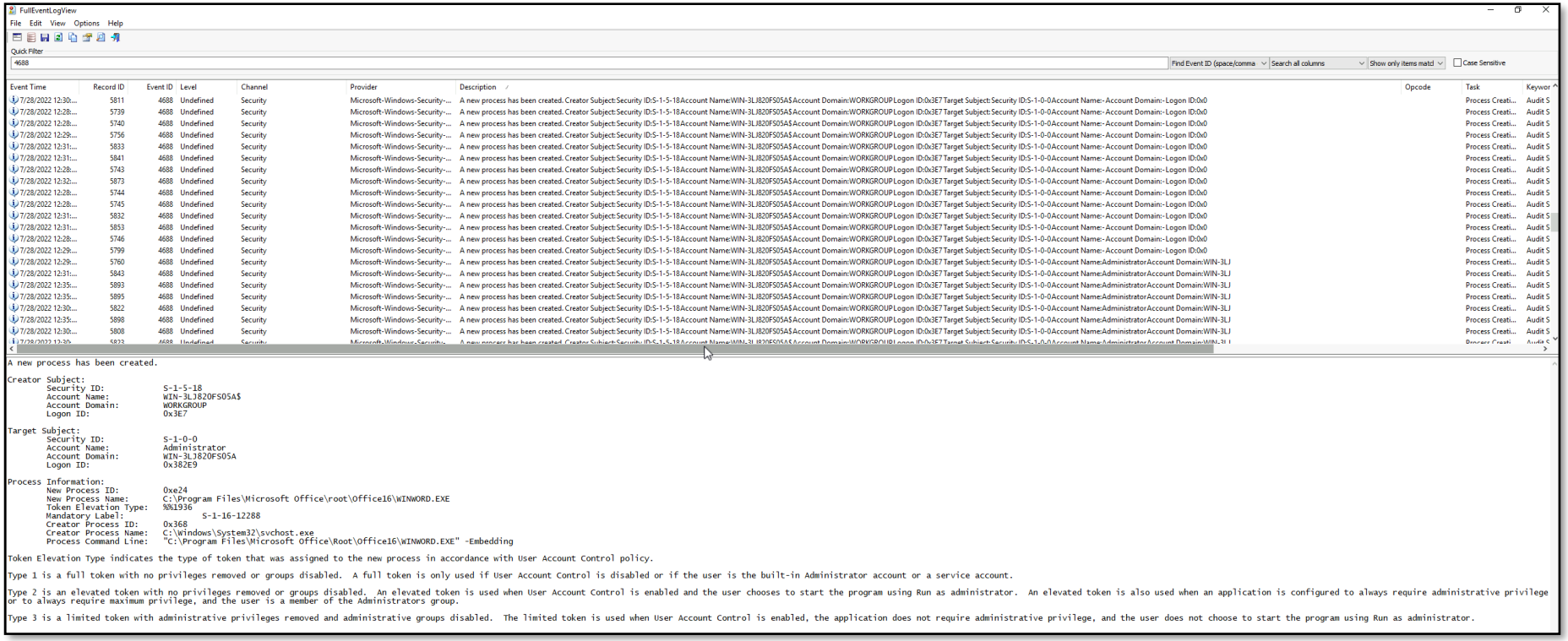
Ao percorrer os processos, você poderá identificar imediatamente o **WINWORD.EXE**, seguido por um processo filho **msdt.exe**. Em algum lugar da lista de processos você também poderá ver um processo para a calculadora que é o **win32calc.exe**.



Para replicar a implementação de "**zero click**" dessa vulnerabilidade, basta salvá-la no formato Rich Text Format (RTF), e estamos prontos para começar. Claro, essa implementação pressupõe que a máquina da vítima esteja no modo de pré-visualização. Essa vulnerabilidade é especialmente preocupante porque, ao contrário da maioria dos malwares, **a vítima não precisa habilitar macros do Office para que o código malicioso seja executado**. É isso que torna a técnica de execução remota de código "zero-click" quase impossível de detectar.

Apesar de não abrir o arquivo, o exploit é executado da mesma forma. Isso acontece por causa de duas características principais:

1) A função do File Explorar de pré-visualizar arquivos antes de abri-los, e
2) O RTF que permite a pré-visualização de arquivos de documentos no File Explorar antes de serem abertos (entre outras finalidades).



Threat hunting

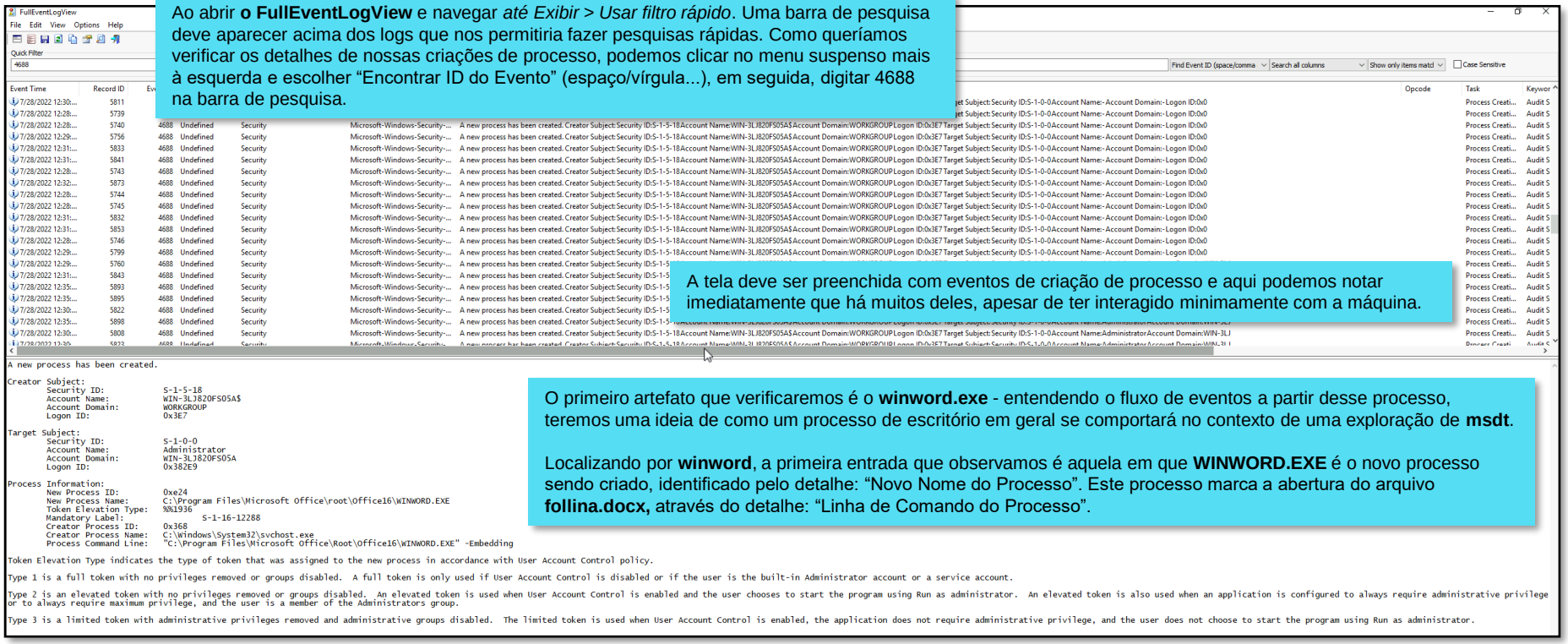
A máquina Windows que usamos para estudar a exploração da vulnerabilidade foi pré-configurada para ter o registro habilitado para:

- Criação de processo de auditoria
- Auditoria de processos em linha de comando, e
- Registro de bloco de script

Dica: Esses mecanismos de auditoria **não estão configurados por padrão** e, como tal, é imperativo que eles sejam ativados em seus próprios ambientes para ajudar na detecção de comportamento suspeito e para ajudar a manter dados valiosos disponíveis para examinadores forenses.

Para esta tarefa, usaremos o **Visualizador de Log de Eventos do Windows** da **Nirsoft** para verificar as criações de processo que identificamos anteriormente. Em seguida, procuraremos detalhes dentro dessas criações de processo que possamos usar para procurar pistas em outros logs de eventos para explicar melhor o que aconteceu nos bastidores.

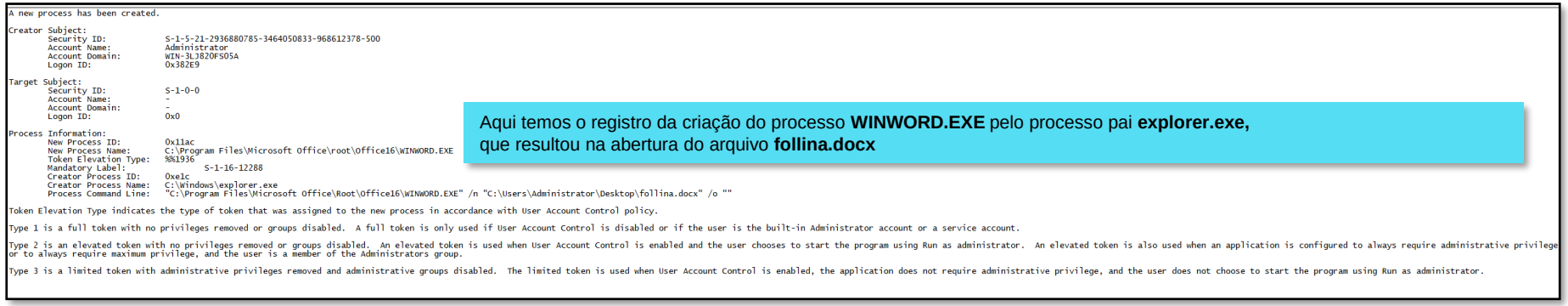
Ao abrir **o FullEventLogView** e navegar *até Exibir > Usar filtro rápido*. Uma barra de pesquisa deve aparecer acima dos logs que nos permitiria fazer pesquisas rápidas. Como queríamos verificar os detalhes de nossas criações de processo, podemos clicar no menu suspenso mais à esquerda e escolher “Encontrar ID do Evento” (espaço/vírgula...), em seguida, digitar 4688 na barra de pesquisa.



A tela deve ser preenchida com eventos de criação de processo e aqui podemos notar imediatamente que há muitos deles, apesar de ter interagido minimamente com a máquina.

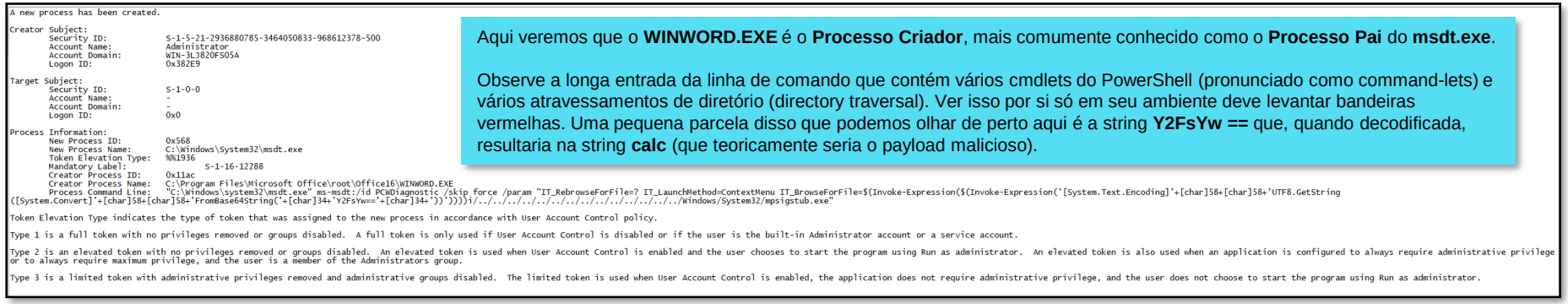
O primeiro artefato que verificaremos é o **winword.exe** - entendendo o fluxo de eventos a partir desse processo, teremos uma ideia de como um processo de escritório em geral se comportará no contexto de uma exploração de **msdt**.

Localizando por **winword**, a primeira entrada que observamos é aquela em que **WINWORD.EXE** é o novo processo sendo criado, identificado pelo detalhe: “Novo Nome do Processo”. Este processo marca a abertura do arquivo **follina.docx,** através do detalhe: “Linha de Comando do Processo”.



```
A new process has been created.

Creator Subject:
        Security ID:            S-1-5-21-2936880785-3464050833-968612378-500
        Account Name:           Administrator
        Account Domain:         WIN-3LJ820FS05A
        Logon ID:               0x382E9

Target Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Process Information:
        New Process ID:         0x11ac
        New Process Name:       C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
        Token Elevation Type:   %%1936
        Mandatory Label:                S-1-16-12288
        Creator Process ID:     0xe1c
        Creator Process Name:   C:\Windows\explorer.exe
        Process Command Line:   "C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\Administrator\Desktop\follina.docx" /o ""

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator.  An elevated token is also used when an application is configured to always require administrative privilege
or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled.  The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
```

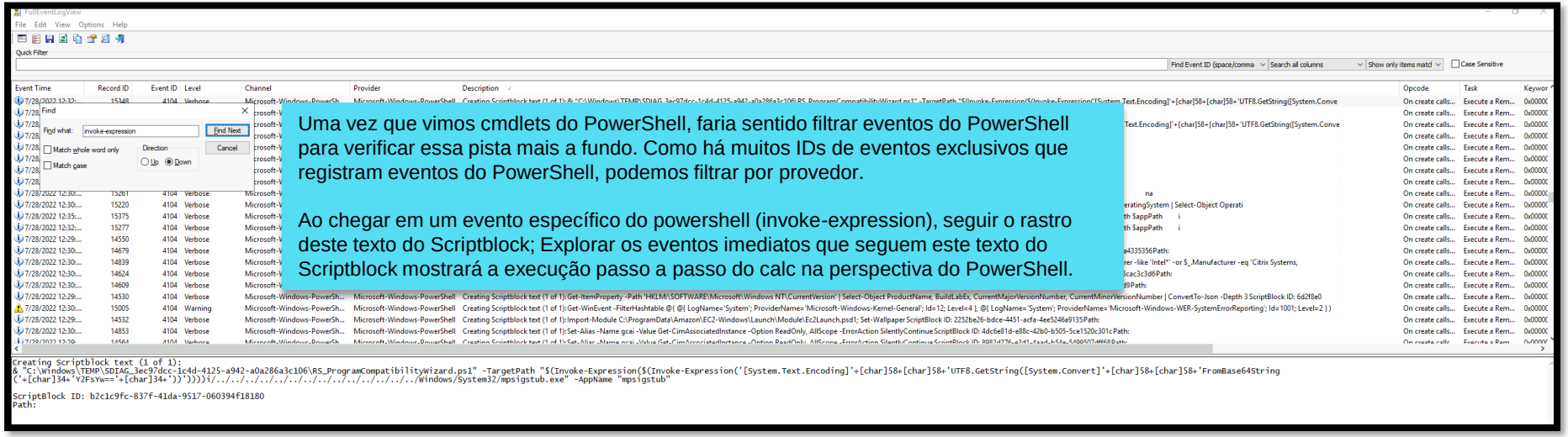
Aqui temos o registro da criação do processo **WINWORD.EXE** pelo processo pai **explorer.exe,** que resultou na abertura do arquivo **follina.docx**



```
A new process has been created.

Creator Subject:
        Security ID:            S-1-5-21-2936880785-3464050833-968612378-500
        Account Name:           Administrator
        Account Domain:         WIN-3LJ820FS05A
        Logon ID:               0x382E9

Target Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Process Information:
        New Process ID:         0x568
        New Process Name:       C:\Windows\System32\msdt.exe
        Token Elevation Type:   %%1936
        Mandatory Label:                S-1-16-12288
        Creator Process ID:     0x11ac
        Creator Process Name:   C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
        Process Command Line:   "C:\Windows\system32\msdt.exe" ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString
([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'Y2FsYw=='+[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe"

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator.  An elevated token is also used when an application is configured to always require administrative privilege
or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled.  The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.
```

Aqui veremos que o **WINWORD.EXE** é o **Processo Criador**, mais comumente conhecido como o **Processo Pai** do **msdt.exe**.

Observe a longa entrada da linha de comando que contém vários cmdlets do PowerShell (pronunciado como command-lets) e vários atravessamentos de diretório (directory traversal). Ver isso por si só em seu ambiente deve levantar bandeiras vermelhas. Uma pequena parcela disso que podemos olhar de perto aqui é a string **Y2FsYw ==** que, quando decodificada, resultaria na string **calc** (que teoricamente seria o payload malicioso).




```
C:\Users\Administrator\Desktop>reg query HKEY_CLASSES_ROOT\ms-msdt

HKEY_CLASSES_ROOT\ms-msdt
    (Default)    REG_SZ    URL:ms-msdt
    EditFlags    REG_DWORD    0x200000
    URL Protocol    REG_SZ

HKEY_CLASSES_ROOT\ms-msdt\shell

C:\Users\Administrator\Desktop>reg export HKEY_CLASSES_ROOT\ms-msdt ms-msdt_backup
The operation completed successfully.

C:\Users\Administrator\Desktop>reg delete HKEY_CLASSES_ROOT\ms-msdt /f
The operation completed successfully.

C:\Users\Administrator\Desktop>reg query HKEY_CLASSES_ROOT\ms-msdt
ERROR: The system was unable to find the specified registry key or value.

C:\Users\Administrator\Desktop>
```

Desabilite o Protocolo MSDT URL

Antes da introdução do patch, as equipes de segurança pressionaram os administradores de TI de suas organizações para desativar imediatamente o Protocolo de URL MSDT. Ao desativar o Protocolo de URL MSDT, os solucionadores de problemas não serão iniciados como links e, portanto, o ms-msdt não poderá ser chamado pelo Office.

Para desativar o protocolo, primeiro execute um prompt de comando como administrador e execute os códigos ao lado <-