FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

Gabriel Servantes
Rafael Rodrigues da Silva

COMO ATIVADORES AFETAM A SEGURANÇA E ESTABILIDADE DO WINDOWS

Americana, SP
2022

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI
Curso Superior de Tecnologia em Segurança da Informação

Gabriel Servantes
Rafael Rodrigues da Silva

COMO ATIVADORES AFETAM A SEGURANÇA E ESTABILIDADE DO WINDOWS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Msc. Maxwell Vitorino

Área de concentração: Segurança da Informação

Americana, SP.
2022

Fatec Americana Ministro Ralph Biasi

Centro Paula Souza 50 anos

SÃO PAULO GOVERNO DO ESTADO

Faculdade de Tecnologia de Americana

Gabriel Servantes
Rafael Rodrigues da Silva

Como ativadores afetam a segurança e estabilidade do Windows

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CETEEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 14 de Junho de 2023.

Banca Examinadora:

Msc Maxwel Vitorino da Silva (Presidente)
Faculdade de Tecnologia – FATEC Americana

Msc Wagner Siqueira Cavalcante
Faculdade de Tecnologia – FATEC Americana

Esp Márcio Roberto Baldo Taglietta
Faculdade de Tecnologia – FATEC Americana

Como ativadores afetam a segurança e estabilidade do *Windows*
How activators affect security and stability in Windows

Gabriel Servantes[1]
Rafael Rodrigues da Silva [2]
Orientador: Maxwel Vitorino da Silva[3]

RESUMO

Ativadores ilegais no *Windows* são programas que permitem aos internautas usarem o sistema operacional sem pagar a taxa de licenciamento. Esses programas são geralmente distribuídos gratuitamente na Internet e são extremamente fáceis de usar. Embora seja ilegal usar um ativador para obter o *Windows* sem pagar, muitas pessoas o fazem porque é mais barato e mais fácil do que comprar uma licença válida. No entanto, existem alguns riscos associados ao uso de ativadores ilegais. Primeiro, eles podem conter *malware* que pode danificar o computador. Segundo os dados podem ser roubados e vendidos por criminosos. Terceiro, sua licença pirata pode deixar de ser válida após uma atualização do *Windows* pois a Microsoft está constantemente bloqueando licenças vazadas ou pirateadas. Atualmente muitos influenciadores e *youtubers* que não entendem sobre segurança ou sobre *Windows*, incentivam a pirataria mesmo sabendo que isso é crime, e que pode levar a problemas para as empresas que os utilizam e para usuários finais, que na maioria das vezes são leigos e não compreendem a natureza da situação em que estão se envolvendo. Sendo assim, uma das possíveis ações a serem tomadas seria as próprias plataformas da Internet banirem este tipo de conteúdo, mas infelizmente isso não acontece, pois para o Google, por exemplo, o que importa é a quantidade de visualizações que os *sites* ou vídeos têm, e não a qualidade deles.
Palavras-chave: Ativadores ilegais, *Windows*, *Malware*s, Segurança da Informação.

ABSTRACT

Illegal Windows activators are programs that allow Internet *users to use the operating system without paying a licensing fee. These programs are generally freely distributed over the* Internet *and are extremely easy to use. While it's illegal to use an activator to get Windows without paying, many people do it because it's cheaper and easier than buying a valid license. However, there are some risks associated with using illegal activators. First, they can contain malware that can harm your computer. Second your data can be stolen and sold by criminals. Third, your pirated license may no longer be valid after a Windows update as Microsoft is constantly blocking leaked or pirated licenses. Currently, many influencers and youtubers who do not understand about security or Windows, encourage piracy even knowing that this is a crime, and that it can lead to problems for companies that use it and the end users themselves, who most of the time are laymen and They don't understand what they're getting into. Therefore, one of the possible actions to be taken would be for the* Internet *platforms themselves to ban this type of content, but unfortunately this does not happen because for google, for example, what matters is the number of views that the sites or videos have, and not their quality.*
Keywords: *Illegal Activators, Windows, Microsoft, Malwares, Information security.*

[1,2,3] Faculdade de Tecnologia, Americana - SP
[1] E-mail: rafael.silva596@fatec.sp.gov.br
[2] E-mail: gabriel.servantes@fatec.sp.gov.br
[3] E-mail: maxwel.silva5@fatec.sp.gov.br

1. INTRODUÇÃO

Segundo Minerbo (2020), em 2010, o IDC (International Data Corporation) mostrou que o *Windows* Server possuía 73,9% do mercado, enquanto o Linux tinha apenas 21,2%, tornando o *Windows* um dos sistemas operacionais mais utilizados e populares em todo o mundo.

Essa popularidade pode ser atribuída, em grande parte, à sua facilidade de uso e ampla compatibilidade com *softwares* e *hardwares*. No entanto, essa popularidade também traz consigo um lado negativo: o *Windows* é frequentemente alvo de ataques cibernéticos e pirataria. Esses problemas, não apenas colocam em risco a segurança dos dados dos usuários, mas também podem resultar em prejuízos financeiros significativos para empresas e indivíduos. Neste artigo, serão abordadas as consequências de se utilizar maneiras ilegais para ativar o *Windows* e como isso afeta a segurança do usuário.

A pirataria de algum sistema é um problema grave, pois resulta em perdas financeiras significativas para a empresa proprietária do sistema. Quando o sistema é ativado de forma ilegal, a proprietária não recebe a devida compensação pelo seu produto. Além disso, muitos usuários que optam por ativar o produto ilegalmente, recorrem a *softwares* de terceiros, como *scripts* e ativadores, que prejudicam a segurança do sistema. No caso de sistemas *Windows*, esses ativadores exigem que o usuário desabilite o antivírus ou o *Windows* update, colocando em risco a segurança do sistema e dos dados do usuário. Além disso, ao desativar esses recursos, o usuário fica impossibilitado de receber atualizações que corrigem falhas e vulnerabilidades no sistema, tornando-o mais suscetível a ataques de vírus e outras ameaças. Portanto, a pirataria do *Windows* não apenas prejudica a Microsoft financeiramente, mas também representa um risco significativo para a segurança do usuário.

Quando um usuário decide ativar o sistema operacional de forma ilegal, muitas vezes recorre à Internet em busca de informações. Infelizmente, existem muitos s*ites* de pirataria e até mesmo vídeos de *youtubers* e influenciadores que ensinam como baixar e utilizar esses *softwares* ilegais. Algumas dessas fontes oferecem versões modificadas do próprio *Windows*, prometendo melhorias milagrosas de desempenho e até mesmo a ativação prévia do sistema. No entanto, o internauta ingênuo pode acabar baixando e utilizando esses *softwares* sem saber que está colocando a segurança de seus dados em risco. Isso ocorre porque esses ativadores geralmente modificam o *Windows* e permitem que criminosos

acessem o computador e os dados do usuário. O problema da pirataria de *Windows* é ainda mais grave quando se considera que muitas lojas se apresentam como "oficiais" e vendem licenças de *Windows* mais baratas. O que muitos usuários não sabem é que essas licenças são, na verdade, pirateadas. Os fornecedores dessas licenças são frequentemente terceiros e não são revendedores oficiais da Microsoft, o que significa que muitas pessoas acabam comprando licenças falsas pensando que estão legalizando suas empresas ao utilizar o produto original. Na realidade, o *Windows* ainda continua sendo pirata, o que pode levar a problemas legais e de segurança para a própria empresa.

No Brasil, é comum encontrar pessoas que usam *softwares* piratas. Isso acontece porque muitos usam a justificativa de que os programas são caros e a maioria das pessoas não tem condições de pagar pelo original, quando na prática a pirataria acontece muito mais por mal hábito já que até mesmo antivírus de US$ 2,99 são pirateados. Além disso, é fácil encontrar s*ites* que oferecem *downloads* de programas piratas.

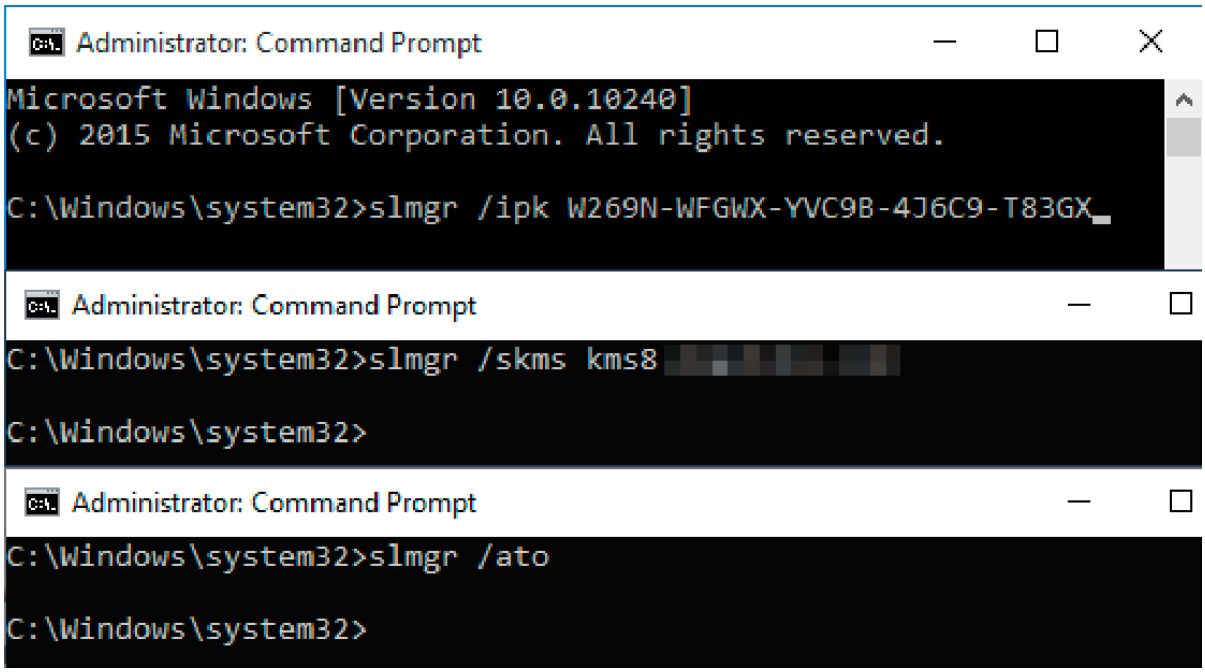
Desde que o YouTube foi criado, em 2005, ele se tornou um dos principais s*ites* de compartilhamento de vídeos do mundo. E, como todo s*ite* popular, o YouTube tem seus problemas. Um deles é o fato de que alguns *youtubers* incentivam a pirataria do *Windows* e de todo tipo de programa, principalmente jogos. Isso é feito de várias maneiras, desde o simples compartilhamento de *links* para s*ites* de *download* ilegais, até tutoriais de como ativar um programa ilegalmente. Em resumo, eles não se importam com os problemas de segurança e estabilidade que isto causará no computador do usuário pois eles ganham dinheiro com os anúncios que são exibidos nos vídeos e isso os motiva a continuar incentivando a pirataria.

2. ATIVAÇÃO DO *WINDOWS*

A ativação via KMS (Key Management Service) do *Windows* é um método usado pela Microsoft para ativar licenças de volume do sistema. Em vez de inserir uma chave de produto individualmente em cada computador, as organizações podem usar o KMS para ativar vários dispositivos em rede usando um servidor KMS central.

Na figura 1, pode-se observar a representação da ativação via KMS usando um servidor não autorizado.

Figura 1: Ativação KMS

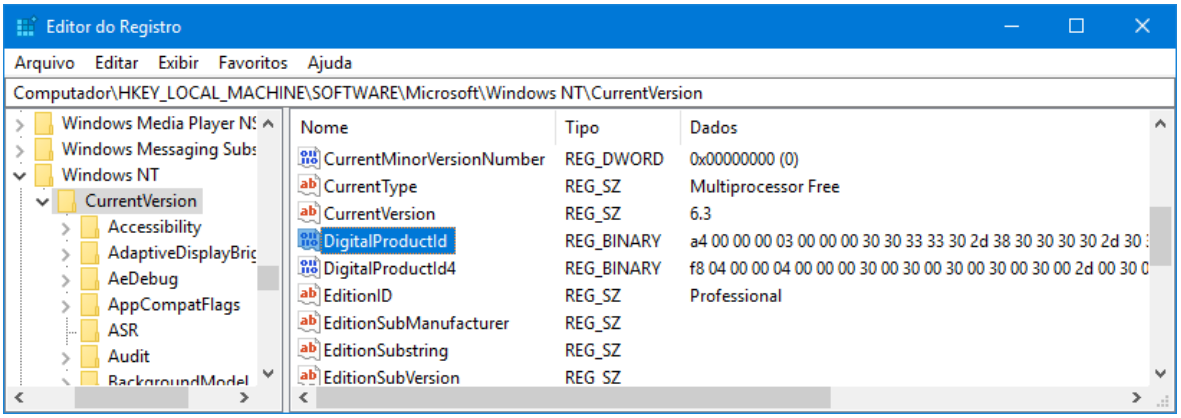


Fonte: Msguides (2023)

Segundo Minerbo (2020), a chave de ativação do *Windows* é um código alfanumérico de 25 caracteres que é usado para validar a licença do *Windows*. Quando o *Windows* é ativado, a chave de ativação é armazenada no Registro do sistema operacional, em uma variável chamada ***DigitalProductId***, que fica dentro da chave HKEY_LOCAL_MACHINE*SOFTWARE*\Microsoft*Windows* NT\CurrentVersion. Essa chave é codificada, mas não criptografada. Dessa forma, qualquer programa ou *script* que queira exibir a chave de ativação precisará decodificá-la para mostrar o resultado.

Na figura 1, pode-se observar a variável ***DigitalProductID*** armazenada no registro do *Windows*:

Figura 2: Variável DigitalProductID no registro do *Windows*



Fonte: Minerbo (2020)

Após o *Windows* ser ativado e a chave armazenada no registro do sistema operacional, o próprio sistema funde a chave genérica com o ***hardware id*** do computador, tornando desnecessário que o usuário insira novamente a chave no mesmo computador. Isso só será possível se a chave estiver atrelada a uma credencial da Microsoft, sendo ela *Outlook, Hotmail, Live* etc.

2.1 ATIVADORES ILEGAIS

Os ativadores de *Windows* são *script*s ou programas que ativam o sistema operacional *Windows* de forma ilegal. Esses programas geralmente são baixados a partir de s*ites* que oferecem versões piratas do *Windows*. Uma vez que o ativador é instalado, ele pode causar vários problemas no computador, incluindo a instabilidade e lentidão do sistema e até mesmo a perda de dados. Além disso, eles podem ser usados por criminosos para obter acesso não autorizado ao computador e roubar informações pessoais.

O tipo mais comum de *malware* contido nos ativadores é o cavalo de Troia. Eles podem ser usados para roubar informações pessoais, instalar outros *softwares* maliciosos ou até mesmo excluir arquivos importantes. Outro tipo bem comum de *malware* encontrado neste tipo de programa são os *spywares* e *backdoors*.

Cavalos de Troia são programas maliciosos que executam ações não autorizadas pelo usuário. Entre essas ações estão excluir, bloquear, modificar ou copiar dados e atrapalhar o bom desempenho dos computadores ou das redes. Diferentemente dos vírus e

worms de computador, os cavalos de Troia não são capazes de se auto propagar (KASPERSKY, 2021).

Segundo a Kaspersky (2021), como o nome sugere, o *spyware* é definido de maneira geral e imprecisa como um *software* destinado a coletar dados de um computador ou outro dispositivo, e encaminhá-los a terceiros sem o consentimento ou o conhecimento do usuário.

2.2 COMO ATIVADORES MODIFICAM O *WINDOWS*

Os principais ativadores encontrados na Internet realizam a ativação via KMS (*Key Management Service*) que é uma tecnologia da Microsoft, usada para ativar produtos da empresa, como o *Windows* e o *Office*. A ativação via KMS envolve o uso de um servidor KMS, que é configurado com uma chave de ativação para ativar os clientes que se conectam a ele.

Ao executar um desses ativadores, ele realizará todo tipo de modificação nos arquivos do *Windows*, incluindo o seu registro, que é um banco de dados hierárquico usado pelo sistema operacional para armazenar configurações e informações importantes do sistema, como configurações do *hardware*, *software* instalado, perfis de usuário e outras configurações. O ativador comumente também adiciona certificados digitais no *Windows* para que *malwares* possam ser considerados como legítimos, facilitando assim o trabalho dos criminosos. Além de modificar o registro do *Windows*, o ativador também deleta chaves do registro, adiciona novas entradas com funções desconhecidas e alteram a permissão de modificação de arquivos protegidos pelo sistema operacional, fazendo com que esses arquivos possam ser modificados facilitando que os *malwares* tenham acesso a áreas que antes não eram possíveis de ser acessadas.

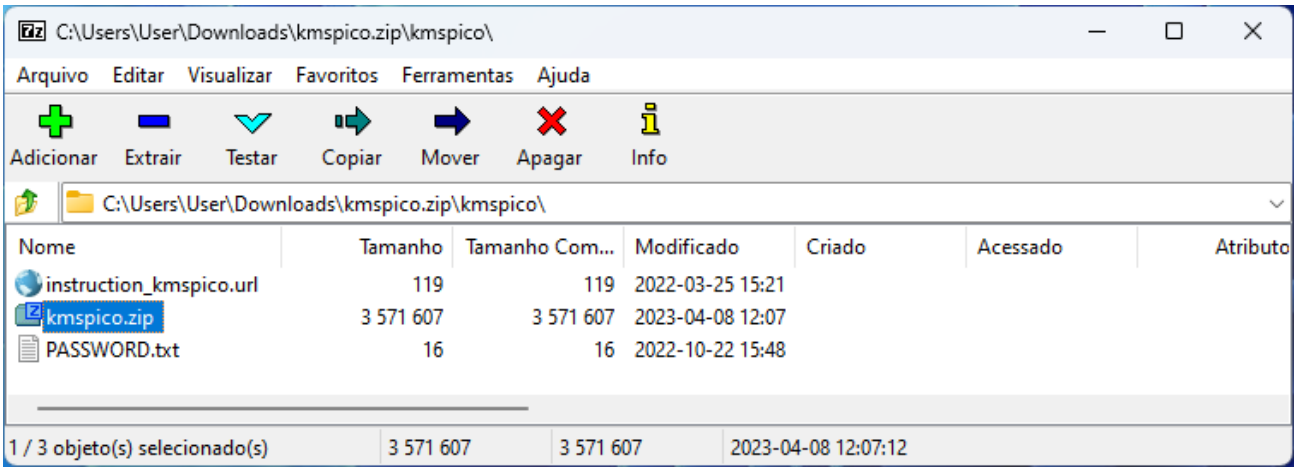
3 REALIZANDO TESTES COM ATIVADOR

Para realizar testes com um ativador comum encontrado na Internet, foi utilizado o *VMware Workstation Pro* para criar uma máquina virtual, garantindo que nenhum *malware* infecte o computador *host*. Foi instalada a versão mais recente do *Windows* 11 nesta máquina virtual e executado o *Windows Update* para garantir a aplicação das últimas correções de segurança. A fim de preservar o ponto inicial da máquina, foi criado um *snapshot*, possibilitando a execução de outros testes a partir deste momento em específico.

3.1 TESTANDO ATIVADOR *KMSPICO*

Inicialmente foi utilizado o *Google* para encontrar um s*ite* com uma das versões deste ativador. Foi feito o *download* em uma página da *web* onde notam-se dois arquivos **kmspico.zip** que está protegido por senha, pois desta forma o antivírus não consegue analisar os arquivos que estão ali, e **password.txt** que armazena a senha para descompactar os arquivos. Na figura 3 é possível observar esses arquivos:

Figura 3: Arquivos “kmspico.zip” e “PASSWORD.txt”



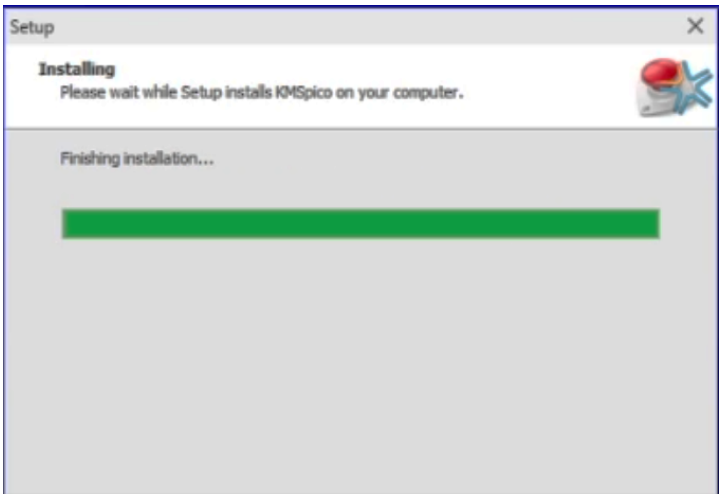
Fonte: próprio autor

Para garantir que nenhum arquivo fosse detectado durante a execução, foi desabilitada a Internet da máquina virtual e a proteção em tempo real do *Windows Defender.*

Foi escolhido o programa *RegShot*, que cria um *snapshot* do registro do *Windows* antes e depois da execução de um programa e as compara mostrando as modificações realizadas, para saber quais as modificações que o *KMSpico* fará no *Windows*. Foi executado o *RegShot* e criando o primeiro *snapshot* do registro antes da execução do ativador.

Na figura 3, observa-se a instalação do *KMSpico* após realizar o primeiro *snapshot*:

Figura 4: Instalação do KMSpico



Fonte: Próprio autor

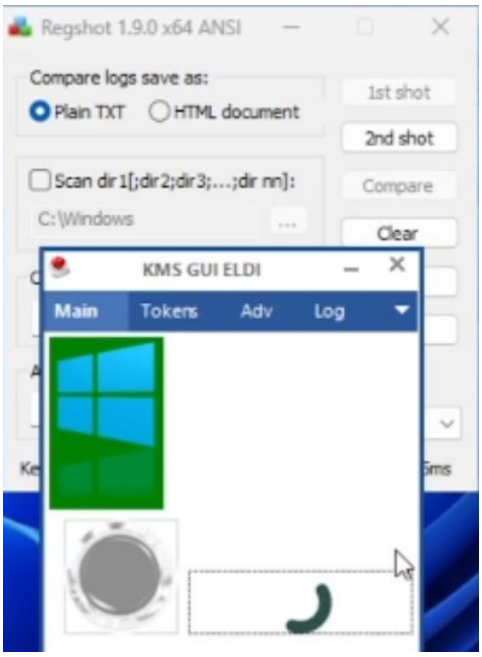
Um detalhe é que no fim da instalação, o próprio *Windows Defender* já detectou o ativador como sendo “HackTool:Win32/AutoKMS” que, segundo a Kaspersky (2016), é uma ferramenta utilizada para criar usuários ocultos no computador, dar permissão a eles, alterar o registro do *Windows*, ocultar usuários maliciosos, analisar pacotes de rede para realizar ações e configurar ataques em computadores locais ou remotos. Na figura 5, observa-se a detecção feita ao final da instalação do ativador.

Figura 5: Detecção do HackTool

Fonte: Próprio autor

Após a instalação, o ativador foi executado na máquina e, posteriormente, o segundo *snapshot* foi criado através do *RegShot*. Na figura 6, observa-se o momento da execução do ativador.

Figura 6: Execução do ativador



Fonte: Próprio autor

Após a criação do segundo *snapshot,* o *RegShot* retornou um *log* com as modificações completas realizadas no sistema durante o intervalo de tempo da execução do ativador.

Na figura 7, observa-se que foram realizadas mais de 400 mudanças desconhecidas no registro do *Windows*.

Figura 7: Total de modificações do registro do *Windows*

```
---------------------------
Total changes: 472
---------------------------
```

Fonte: Próprio autor

Na figura 8, observa-se que, em meio a outras mudanças no registro, o ativador modificou especificamente o conteúdo do registro ***SoftwareProtectionPlatform***, que armazena informações relacionadas à ativação do *Windows* e do *Office* no sistema operacional e a mudança deste registro faz com que seja possível “enganar” a ativação do *Windows* e *Office*.

Figura 8: Chaves adicionadas

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\55c92734-d6
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\55c92734-d6
HKLM\SOFTWARE\Microsoft\AudioCompressionManager
```

Fonte: Próprio autor

Na figura 9, observa-se que a proteção ***SmartScreen*** foi desativada, significando que o *Windows* não conseguirá verificar os aplicativos que estão sendo executados, bem como, verificar arquivos baixados da Internet, isso facilita muito a execução de *malwares* no computador e possibilita que o ativador baixe outros vírus na Internet e execute na máquina do usuário.

Figura 9: *SmartScreen* desativado

```
-------------------------------
Values added: 328
-------------------------------
HKLM\SOFTWARE\Microsoft\Internet Explorer\PhishingFilter\EnabledV9: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\PerfMMFileName: "Global\MMF BITS
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SmartScreenEnabled: "Off"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1708\Terminator:
```

Fonte: Próprio autor

Na figura 10, é constatado que o ativador adiciona novos certificados digitais ao *Windows*, o que permite que *softwares,* que antes seriam considerados perigosos, agora passam a ser legítimos, pois o ativador instalou um certificado que engana o sistema e faz com que ele pense que um vírus é inofensivo, permitindo que ele tenha total autonomia para infectar o computador do usuário.

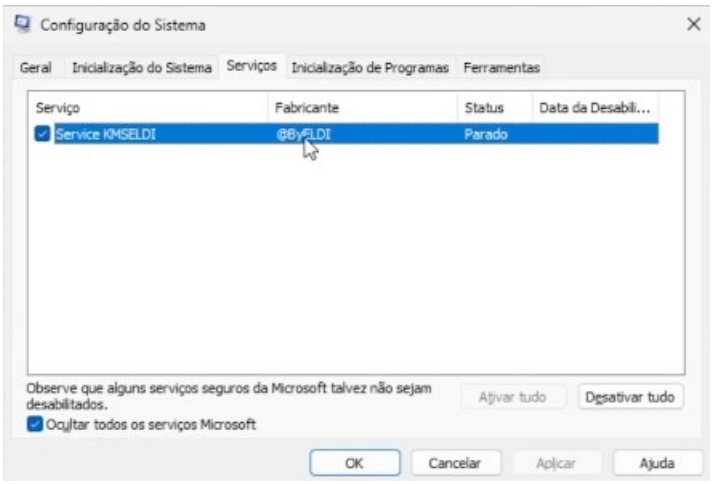
Figura 10: Certificados desconhecidos adicionados

```
---------------------------------
Values modified: 85
---------------------------------
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\ProductId: "00330-80000-00000-AA183"
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\ProductId: "00331-10000-00001-AA535"
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\DigitalProductId:  A4 00 00 00 03 00 00 00 30
30 33 33 30
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\DigitalProductId:  A4 00 00 00 03 00 00 00 30
30 33 33 31
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration\DigitalProductId4:  F8 04 00 00 04 00 00 00 30
00 33 00 3
HKLM\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\BE36A4562FB2EE05DBB3D323
23ADF445084ED656\Blob:  0F
HKLM\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\BE36A4562FB2EE05DBB3D323
23ADF445084ED656\Blob:  5C
```

Fonte: Próprio autor

Na figura 11, observa-se que o ativador adicionou um serviço criado pelo autor, “@ELDI”, e,através deste serviço, o criminoso pode executar comandos até mesmo antes do *Windows* ser iniciado, fazendo com que o ataque seja ainda mais danoso para o usuário, podendo ocasionar todo tipo de problema, como vazamento de dados, lentidão, problemas no *boot* do *Windows,* etc.

Figura 11: Serviço KMSELDI desconhecido criado

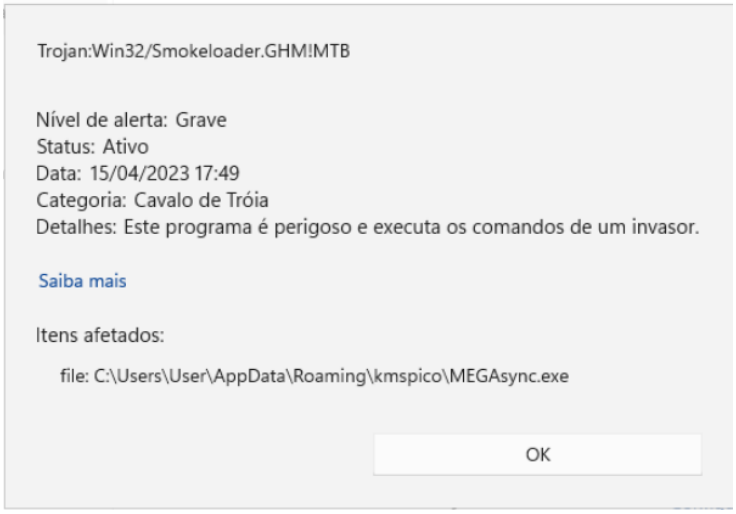


Fonte: Próprio autor

O ativador também criou os arquivos “ewxck”, “MEGAsync.exe” e “*Script*.vbs”, onde o executável “MEGAsync.exe” foi detectado pelo próprio *Windows Defender* indicando que na verdade se tratava de um *trojan,* chamado “Smoke Loader” (Figura 13), conhecido por proliferar vários outros vírus, ao ser executado pelo usuário, ele se conecta na Internet e baixa a versão mais recente do *malware* e modifica sua própria data de criação/modificação, dificultando ainda mais sua detecção pelo antivírus, podendo baixar mineradores de criptomoedas na máquina do usuário, tornando a experiência com o *Windows* muito lenta. Nesta etapa é comum o sistema operacional apresentar diversos travamentos e lentidão.

Na figura 12, observa-se que o próprio *Windows Defender* fez uma detecção de um tipo de cavalo de Troia (trojan) que é projetado para infectar sistemas e fornecer acesso remoto não autorizado ao computador infectado. É conhecido como "smokeloader" devido ao nome do arquivo executável que costuma ser utilizado durante a infecção.

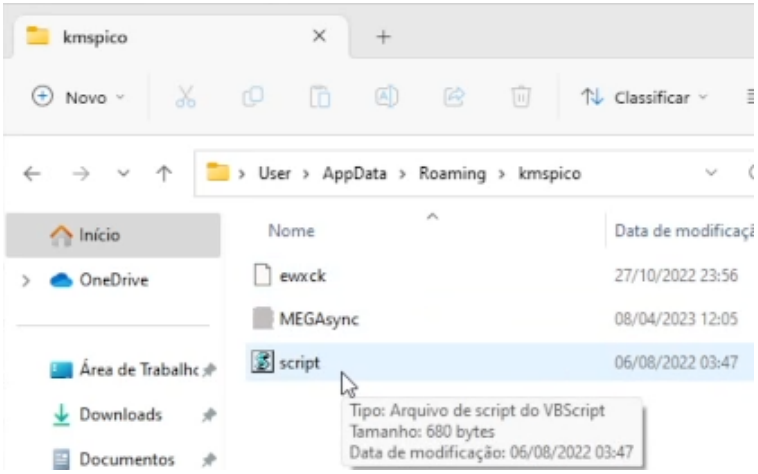
Figura 12: SmokeLoader



Fonte: Próprio autor

Na Figura 13, é possível observar os arquivos gerados após a instalação do ativador. Neste diretório, foram criados três arquivos, sendo um deles um script VBS (Visual Basic Script) malicioso.

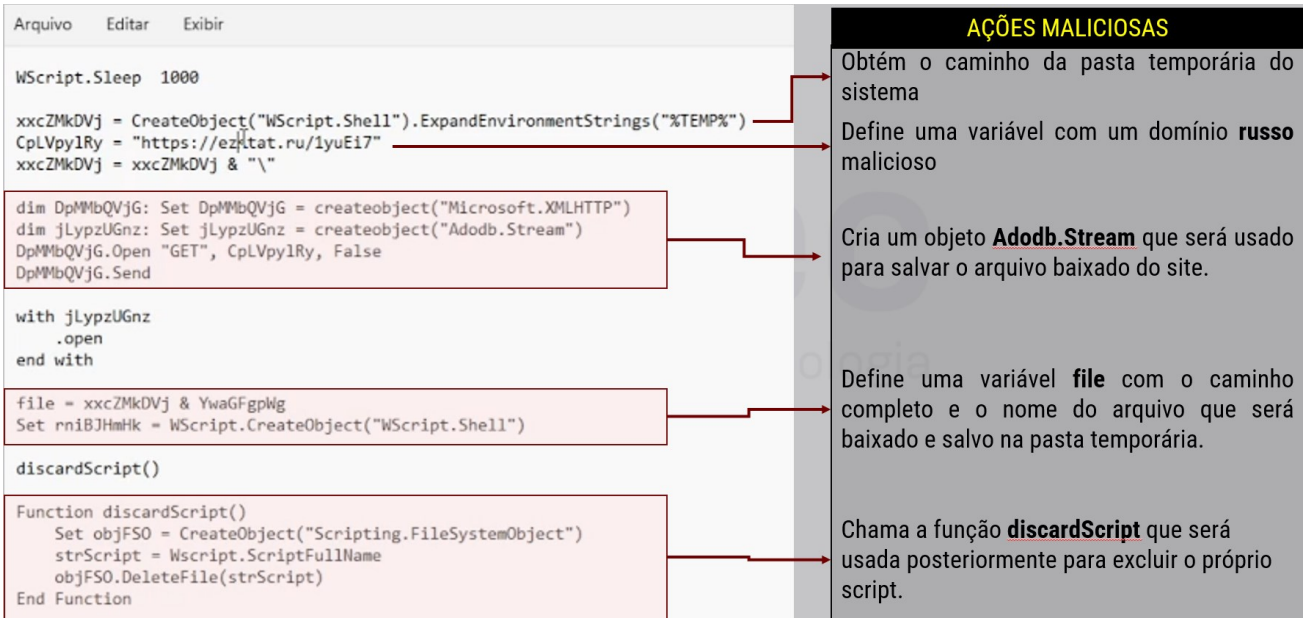
Figura 13: Arquivos criados pelo ativador



Fonte: Próprio autor

Na figura 14, é demonstrado o conteúdo do arquivo “*Script*.vbs” criado pelo ativador. Por se tratar de um *script* em VBS (*Visual Basic Script*) o criminoso é capaz de realizar comandos para baixar arquivos da Internet e executar programas no computador do usuário.

Figura 14: *script* em vbs criado pelo ativador



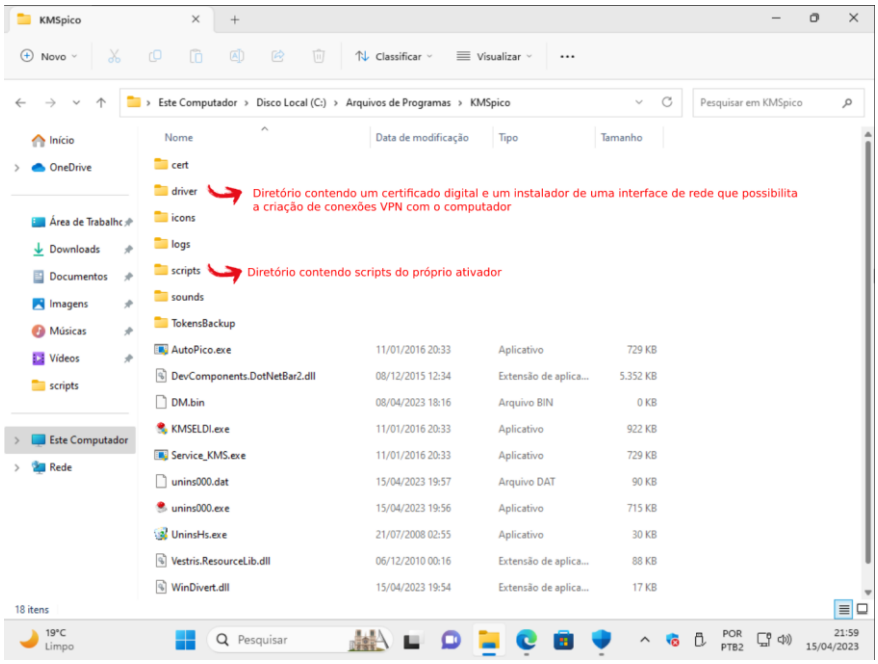
Fonte: Próprio autor

De acordo com o código, a função ‘xxcZMkDVj()’ cria um objeto do *Windows Script Host* (W*Script*.Shell) para obter o caminho da pasta temporária do sistema em que o *script* está sendo executado. Define uma variável ‘CpLVpylRy()’ com o endereço de um s*ite* que será usado posteriormente para baixar um arquivo. Cria um objeto *Adodb.Stream* que será usado para salvar o arquivo baixado do s*ite*. Define uma variável "*file*" com o caminho completo e o nome do arquivo que será baixado e salvo na pasta temporária. Chama a função "discard*Script*" que será usada posteriormente para excluir o próprio *script*.

Em resumo, esse *script* malicioso baixa um arquivo de um *site* específico e o salva na pasta temporária do sistema. Em seguida, o *script* chama a função "*discardScript*", que é usada para excluir o próprio *script* depois que ele é executado, dificultando ainda mais sua detecção.

O ativador utilizado para ativar o sistema operacional *Windows* criou diversas pastas no diretório **C:\Program Files\KMSPICO**. Entre elas, destaca-se a pasta **driver**, observada na figura 15.

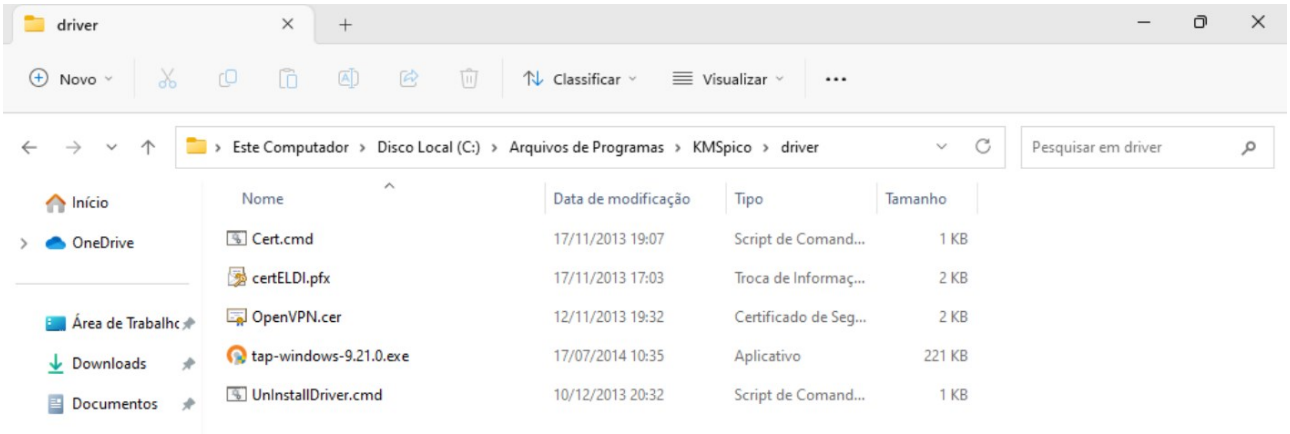
Figura 15 – Diretórios criados na instalação do ativador KMSPICO



Fonte: Próprio autor

Na pasta **driver** observa-se, um certificado digital desconhecido e um instalador de adaptador de rede para o *Windows*, demonstrados na figura 16. Tal adaptador permite a criação de conexões VPN (Virtual Private Network) com a máquina do usuário.

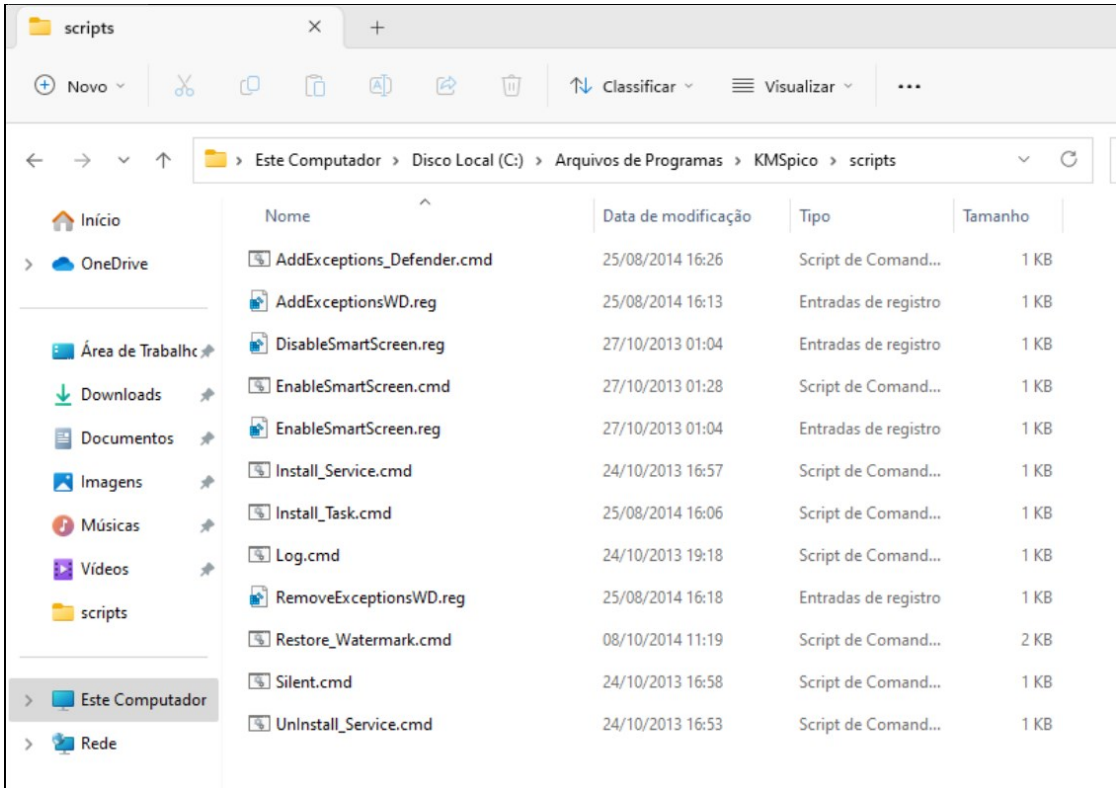
Figura 16: Conteúdo do diretório “drivers”



Fonte: Próprio autor

Além disso, foi identificada a pasta ***script*s**, que contém diversos *script*s (figura 17) capazes de realizar modificações no registro do *Windows*. Essas modificações permitem que *malware*s possam infectar o computador.

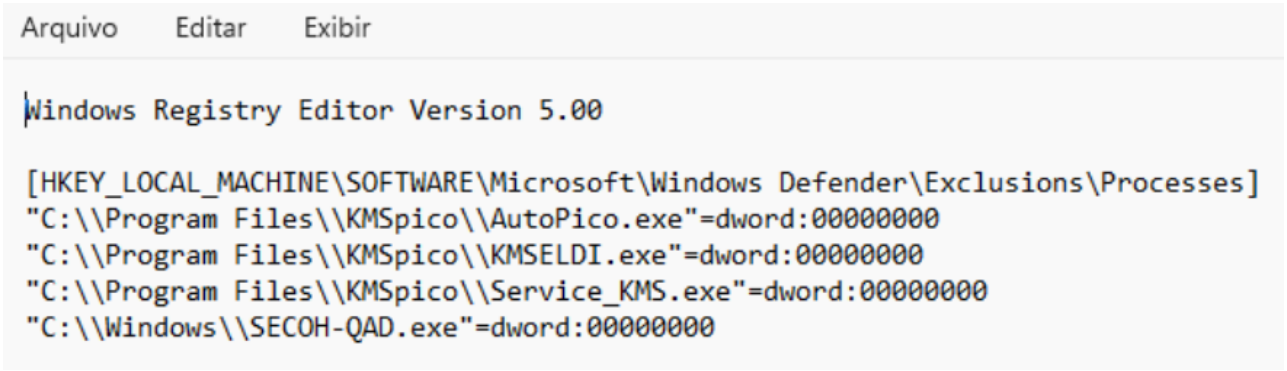
Figura 17: Conteúdo do diretório *script*s



Fonte: Próprio autor

Apenas analisando o conteúdo do arquivo “AddExceptionsWD.reg”, é possível constatar que o ativador realiza mudanças no sistema operacional para poder infectá-lo, uma vez que ele adiciona seus próprios executáveis na lista de exceções do *Windows Defender.* Assim ele poderá realizar qualquer ação no computador do usuário, sem que o antivírus o impeça de agir. Desta maneira o usuário termina com um *Windows* totalmente diferente de como ele estava antes de realizar a ativação e com o agravante de agora estar infectado, podendo ocasionar perda ou vazamento de seus dados. Na figura 18, observa-se o conteúdo de “AddExceptionsWD.reg”.

Figura 18: Conteúdo do arquivo “AddExceptionsWD.reg”



Fonte: Próprio Autor

4 CONSIDERAÇÕES FINAIS

Com o lançamento do *Windows* 11, uma nova versão do sistema operacional da Microsoft, muitos usuários têm buscado formas de adquirir a licença de forma ilegal por meio de ativadores disponíveis na internet. No entanto, este estudo apresentou evidências de que o uso indevido dessas ferramentas pode resultar em sérios danos e problemas de segurança no sistema.

Os testes realizados demonstraram que os ativadores podem permitir que *softwares* problemáticos e até mesmo maliciosos sejam instalados no computador, além de possibilitar a realização de ações desconhecidas que podem acarretar a problemas diversos no sistema operacional. Os resultados também indicaram que a instalação de um ativador pode interferir na estabilidade do sistema operacional e causar falhas que podem prejudicar o desempenho da máquina.

A Microsoft tem trabalhado para desenvolver recursos e medidas de segurança para combater práticas ilegais e proteger seus usuários, e é fundamental que os usuários sigam as recomendações da empresa e adquiram suas licenças de forma legal. Também é importante tomar cuidado com os “gurus da internet” e sempre realizar as devidas pesquisas antes de realizar práticas arriscadas, das quais não se tem conhecimento.

Em conclusão, a obtenção da licença de forma legal é a melhor opção para garantir a segurança e estabilidade do sistema operacional, bem como a proteção das informações do usuário. O uso de ativadores ilegais pode resultar em danos e problemas de segurança significativos, além de infringir a lei de direitos autorais. Portanto, é fundamental que os usuários evitem essa prática e adquiram suas licenças de forma legítima, protegendo assim não só seus sistemas, mas também sua integridade e privacidade pois, afinal de contas, os danos causados por todos os problemas apresentados neste trabalho certamente são muito superiores ao gasto que um usuário terá com uma licença autêntica.

REFERÊNCIAS

ASHISHMOHTA@TWC. ***Software* protection platform service sppsvc.exe causing high CPU usage**. Disponível em: https://www.the*Windows*club.com/*software*-protection-platform-service-causing-high-cpu-usage. Acesso em: 15 abr. 2023.

KASPERSKY. **O que é spyware?** definição. Disponível em: https://www.kaspersky.com.br/resource-center/threats/spyware. Acesso em: 15 nov. 2022.

KASPERSKY. **O que é um cavalo de Troia?** Disponível em: https://www.kaspersky.com.br/resource-center/threats/trojan-virus. Acesso em: 15 nov. 2022.

Kaspersky Threats — **HackTool**. Kaspersky.com. [S.l]. Disponível em: https://threats.kaspersky.com/br/class/HackTool/. Acesso em: 15 abr. 2023.

Kaspersky Threats — **Backdoor.Win32.Mokes**. Kaspersky.com [S.l]. Disponível em: https://threats.kaspersky.com/br/threat/Backdoor.Win32.Mokes/. Acesso em: 15 abr. 2023.

MINERBO, Aurélio. **Cuidado:** licença permanente e vitalícia vendida na *web* é golpe. [S.l.]:Baboo, 2021. Disponível em: https://www.baboo.com.br/*Windows*-10/conteudo-essencial-*Windows*/cuidado-licenca-permanente-e-vitalicia-vendida-na-*web*-e-golpe/4/#split_content. Acesso em: 15 nov. 2022.

MINERBO, Aurélio. **Pirataria do *Windows***: a fundo, [S.l.]:Baboo, 2018. Disponível em: https://www.baboo.com.br/*Windows*-10/conteudo-essencial-*Windows*/pirataria-do-*Windows*-a-fundo/. Acesso em: 15 nov. 2022.

MINERBO, Aurélio. **Ativadores de *Windows* a fundo**. Youtube, 15 de novembro de 2022. Disponível em: https://www.youtube.com/watch?v=esu55Q74NU0. Acesso em: 15 nov. 2022.

MINERBO, Aurélio. **Introdução e bobagens dos *youtubers***. *Windows* rápido e seguro. Youtube, 30 jan. 2020. Disponível em: https://www.youtube.com/watch?v=JVbSszdiAhE. Acesso em: 15 nov. 2022.

QUINNRADICH**. Usando o VB*Script* Win32 apps**. Disponível em: https://learn.microsoft.com/pt-br/*Windows*/win32/lwef/using-vb*script*. Acesso em: 16 abr. 2023.

SMILE, Always. **Easy ways to activate *Windows* 11 for FREE without a product key. MS Guides**. Disponível em: https://msguides.com/*Windows*-11. Acesso em: 18 jun. 2023.

TEAM, K. **Brasil é o país mais atacado por ameaça que rouba dados confidenciais**. Disponível em: https://www.kaspersky.com.br/blog/nullmixer-brasil-pais-mais-atacado/20117/. Acesso em: 15 nov. 2022.