Article

Keylogger

Gabriel Bernardes de Moura [1], Henrique Bezerra Lucas [2], Pedro Gabriel Bueno Faria [3], Vinicius Francisco Pinha [1]

[1] Tecnologia em Análise e Desenvolvimento de Sistemas; (Moura) gabrielbemoura@gmail.com, (Faria) pedrobuenofaria16@gmail.com
[2] Engenharia de Computação; (Pinha) viniciuspinha@hotmail.com
[3] Engenharia de Software; (Lucas) henriquelucas@alunos.utfpr.edu.br

Resumo: Nesse artigo, são apresentado os principais conceitos envolvendo keylogger, um tipo de malware que infecta à máquina dos usuários, armazena as informações acessadas pelo usuário, podendo até mesmo vazar elas pela rede. Para observar de forma prática foi construído um keylogger de forma intencional e realizado um experimento simulando uma infecção de uma máquina para analisar as possíveis aplicações e falhas de segurança do sistema.

Palavras-Chave: keylogger; segurança; privacidade; invasão;

1. Introdução

Atualmente, com a utilização de computadores e celulares para armazenar e compartilhar informações surgem novas ameaças para integridade e segurança dos usuários que fazem uso desses meios, existem diversos modos para invadir a privacidade dos usuários, um dos métodos mais antigos e aprimorados é o Keylogger. Essa técnica se baseia, principalmente, no conceito de escutar e copiar as informações recebidas em uma máquina por exemplo, por meio de um teclado. Ao escutar a teclas que são pressionadas no teclado, esse malware consegue replicar o contéudo, salvá-los em um arquivo escondido dentro da própria máquina ou enviá-los para outros usuários utilizando a rede, tudo de forma silenciosa, esse roubo de informações corrobora para o acontecimento de crimes ainda mais graves, além de expor publicamente os usuários de um meio considerado privado.

Para além dos modos mal intencionados de uso, um keylogger pode ser utilizado de forma saudável, por exemplo para supervisão e controle da produtividade de uma empresa por meio da verificação dos dados que cada empregado digita no computador no momento de trabalho. Outro ponto eficaz é no controle parental, pais podem instalar softwares para supervisão do contéudo que seus filhos visitam na internet. Além disso, caso os usuários principais estejam inserindo dados sensíveis a perda, esse método também pode servir para garantir uma cópia em tempo real daquilo que está sendo digitado no computador. Todas essas aplicações do keylogger são feitas de modo privado e sem apresentar riscos para sociedade em geral.

Um dos primerios registros do uso de keylogger para captura e envio de dados de forma ilícita ocorreu durante o período da Guerra Fria, onde espiões da antiga União Soviética implataram em uma série de máquinas datilográficas dos Estados Unidos pequenos circuitos eletromecânicos que detectavam e enviam em tempo real para os soviéticos todas as informações digitadas pelos estadunidenses, o dano causado pelo vazamento se tornou imensurável, tendo em vista que essa espionagem ocorreu sem levantar suspeitas durante 8 anos. Em um contexto atual, as formas de aplicação desse método se sofisticaram e se tornaram ainda mais abragentes podendo afetar qualquer usuário que possua um computador no mundo. De acordo com uma pesquisa divulgada pelo Internet World Stats mais de 5 bilhões de pessoas acessam a internet no mundo, o que implica em uma incrível gama de troca de informações diariamente. Acesso a contas bancárias, compras on-line e números de documentos são algumas das diversas formas de interação com o computador que envolvem a digitação de dados, dessa forma, o envio e salvamento de informações nos

Citation: Moura, Gabriel.; Lucas, Henrique.; Faria, Pedro.; Pinha, Vinicius. Criação de um keylogger. *Appl. Sci.* **2022**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:

computadores deve ocorrer de modo confidencial para garantir a privacidade dos usuários e a segurança dos dados. Nesse quesito, a utilização de um sistema anônimo para gravar as informações digitadas pelos usuários de modo silencioso representa um grave risco de segurança que aumenta conforme o tempo de exposição, uma análise dos dados coletados por esse malware pode, na melhor das perspectivas, expor informações que facilitem a aplicação de futuros golpes.

Além das informações digitadas, esse malware pode incorporar novas ferramentas que aumentam a abrangência dos tipos de dados capturados, o acesso a webcam do usuário para retirar fotos em um determinado intervalo de tempo, realizar um screenshot da tela do computador no momento que um click no mouse é disparado e salvar as querys de pesquisas de outras aplicações são outras modelos de captura que podem ser salvos.

Para verificar o funcionamento e explorar as possíveis falhas de segurança, foi realizado um experimento apresentado nas seções a seguir com a construção de um keylogger para captura das informações digitadas pela máquina na qual ele será instalado e organização dessas informações em um arquivo de texto. Nas próximas seções serão apresentados os resultados obtidos, a metodologia usada para o desenvolvimento do malware e as fontes de informação utilizadas.

As citações devem ser feitas no texto utilizando [**?**] is a set of macros built atop TEX [**?**]. e a bibliografia deve ser incorporada no final deste documento.

2. Materiais e Métodos

Para avaliar esse cenário será criada utilizando a linguagem Java uma interface de interação com um keylogger que infecte a máquina do usuário e gere um arquivo com as informações digitadas. Além da coleta da entrada de dados, a organização dos textos coletados, ou seja, a categorização daquilo que foi coletado de modo a classificar as informações conforme a viabilidade delas é outro ponto essencial que será abordado juntamente com o envio das informações coletadas para outro usuário ou máquina utilizando a internet.

O desenvolvimento deve ser feito de modo iterativo e incremental, para isso será utilizado o Processo Unificado como modelo de ciclo de vida. O ciclo de vida do processo é dividido em 4 fases: Concepção, Elaboração, Construção e Transição, em cada uma dessas fases são desenvolvidos 5 fluxos de trabalho em diferentes graus, sendo eles: Requisitos, Análise, Projeto, Implementação e Teste. Os fluxos de trabalho ocorrem de modo interativo dentro de cada fase, permitindo a análise do que foi produzido e o aperfeiçoamento do projeto de modo contínuo.

Esta seção tem o objetivo de apresentar formalmente o trabalho, seja por meio de linguagem matemática ou de desenhos, fluxogramas, esquemas gráficos, etc. Na segunda parte da seção devem ser discutidos e apresentados quais são as ferramentas utilizadas para solucionar o problema e como elas se relacionam (quando houver mais de uma).

Nesta seção é uma boa tática utilizar-se de figuras para apresentar a proposta de solução do problema.

3. Resultados

Esta seção deve apresentar os resultados, logo **ela só será necessária na versão final do texto**.

3.1. Figuras e Tabelas

Todas as figuras e tabelas devem ser citadas no texto principal seguindo o formato: Figura 1, Tabela 1, Tabela 2, etc.

Figure 1. Esta é a legenda de uma figura. É importante que a legenda complemente e até mesmo repita informações contidas na figura para que fique claro a ideia e o objetivo de apresentá-la. Utilize o \label{alias} para dar nome a figura e referenciá-la posteriormente utilizando \ref{alias}.

Table 1. Esta é a legenda de uma tabela. Ela deve ficar acima da tabela ao contrário das figuras que as legendas ficam após.

Title 1	**Title 2**	**Title 3**
Entry 1	Data	Data
Entry 2	Data	Data

Table 2. Esta é uma tabela mais longa quando há muitas informações a serem colocadas na tabela. Use com parcimônia.

Title 1	**Title 2**	**Title 3**	**Title 4**
Entry 1	Data	Data	Data
Entry 2	Data	Data	Data[1]

[1] This is a table footnote.

4. Conclusões

Aqui vocês irão apresentar as conclusões as quais chegaram após a finalização do trabalho. Na proposta, esta seção deve apresentar as considerações finais e seu nome deve ser alterado para **Considerações Finais**.

Referencias

1. Sagiroglu, Seref e Canbek, Gurol. Increansing Threats to Computer Security and Privacy. *IEEE TECHNOLOGY AND SOCIETY MAGAZINE* **2009**, *FALL*, 10–17.
2. Creutzburg, Reiner. The strange world of keyloggers - an overview, Part I. *Electronic Imaging* **2017**, *pp*, 139–148.
3. Robbi, Rahim. Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm. *IOP Publishing Ltd* **2018**.
5. Internet World Stats. Available online: https://www.internetworldstats.com/stats.htm (acessado em 10/11/2022).
5. How Soviets used IBM Selectric keyloggers to spy on US diplomats. Available online: https://arstechnica.com/information-technology/2015/10/how-soviets-used-ibm-selectric-keyloggers-to-spy-on-us-diplomats/ (acessado em 15/11/2022).