UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

CENTRO DE ENSINO SUPERIOR DO SERIDÓ - CERES/CAICÓ

DEPARTAMENTO DE TECNOLOGIA E COMPUTAÇÃO

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ANDRÉ FELIPE G. M. DE MEDEIROS

HUGO RAFAEL DE MEDEIROS FERNANDES

ROBSON AGRIPINO DA SILVA

RELATÓRIO FINAL DE SEGURANÇA DA INFORMAÇÃO

CAICÓ - RN

2016

ANDRÉ FELIPE G. M. DE MEDEIROS

HUGO RAFAEL DE MEDEIROS FERNANDES

ROBSON AGRIPINO DA SILVA

RELATÓRIA FINAL DE SEGURANÇA DA INFORMAÇÃO

Relatório da disciplina Tópicos Especiais em Segurança da Informação do curso Sistemas de Informação, como parte dos requisitos para obtenção do título de Bacharel em Sistemas de Informação da Universidade Federal do Rio Grande do Norte.

Prof. Tiago dos Santos Bezerra

CAICÓ - RN

2016

Sumário

1 Introdução

Este trabalho faz parte dos requisitos para avaliação da disciplina tópicos especiais em segurança da informação, onde busca apresentar os conceitos adquiridos em sala de aula a respeito dos softwares maliciosos conhecidos como keylogger, como também os resultados obtidos na implementação de uma dessas aplicações.

1.1 Problematica

É importante destacar que malwares como keyloggers não se limitam a uma única plataforma, o que acontece é que a família de sistemas operacionais da microsoft é mais populares entre os usuários, deste forma sendo a mais visadas. Portanto, a plataforma-alvo para a qual o keylogger foi implementado é a Microsoft Windows.

Além disso, os requisitos básicos necessários para a construção desse projeto são que o keylogger deve coletar os dados digitados pelo usuário, esconder sua execução da vítima, poder iniciar durante a inicialização do windows, funcionar em diferentes versões do sistema operacional, como também poder enviar as informações coletadas para o email do atacante.

2 Referencial teórico

A presente seção tem o objetivo de introduzir os conceitos deste trabalho, bem como apresentar as tecnologias utilizadas pela equipe em seu desenvolvimento.

2.1 Segurança da informação

O propósito da segurança da informação é proteger os valiosos recursos de uma organização, tais como informação, hardware e software. Através da aplicação de mecanismos de segurança apropriados, pode-se auxiliar a missão de uma organização, protegendo seus recursos físicos e financeiros, (PELTIER, 2013).

O uso destes mecanismos tem o intuito de prevenir o acesso não autorizado aos dados da empresa, bem como o uso, modificação, destruição ou divulgação destes dados.

2.2 Cyber ataque

A Wikipédia define cyber ataque como qualquer tipo de manobra, empregada por um indivíduo ou organização, que visa sistemas de informação computacional, infra

estruturas, redes de computadores, ou aparelhos pessoais através de diversos meios maliciosos, geralmente originados de uma fonte anônima que pode roubar, adulterar ou destruir um alvo específico, hackeando um sistema suscetível.

São conhecidas diversas formas de cyber ataque entre elas encontram-se o cavalo-de-tróia, phishing, vírus, worms, além dos screenloggers, e keyloggers, este último, sendo o foco deste trabalho.

2.3 Malwares

Os malwares são um dos principais meios usados para a prática ao Cyber Ataque. Também conhecido como vírus de computador, os malwares são em suma nada mais que softwares de intenções maliciosas com objetivos que variam de acordo com o seu propósito, tais como:

- Apagar ou alterar arquivos, afim de prejudicar o funcionamento de um sistema operacional ou um software especifico;
- Monitorar a atividades de um sistema enviar as informações para terceiros;
- Capturar e armazenar as teclas digitadas pelos usuário, usado principalmente para a obtenção de login e senha.

Os vírus de computador recebem esse nome porque possuem, da mesma forma que o vírus biológico, a capacidade de se propagar pelo meio no qual estão inseridos. Seu principal meio de contaminação é através da internet, onde o vírus pode se propagar mais rapidamente e infectar um número maior de computadores. Abaixo estão descritos alguns meios de contaminação explorados:

- **Falhas de segurança (*bugs*)**: Sistemas operacionais e outros softwares que possuem falhas, que quando descobertas, podem ser exploradas para fins maliciosos;
- **E-mails**: os usuários recebem e-mails que tentam induzi-los a executar um arquivo anexado ou presente em um link;
- **Downloads**: usuários podem baixar arquivos que estão infectados de determinados sites;
- **Redes sociais e mensagens instantâneas**: links para vírus também podem ser transmitidos via Facebook, WhatsApp e Twitter.

Alguns tipos de malwares mais conhecidos são: Cavalo de Troia (trojan), Worm (verme), Spyware, Vírus, Rootkit e Keyloggers. Tendo este último como o objetivo deste relatório e será discutido mais detalhadamente na próxima seção.

2.4 Keyloggers

Keyloggers são classificados como softwares maliciosos devido sua capacidade para a espionagem, utilizam o teclado como forma primária para obtenção de informação do usuário, sendo esta a forma mais comum de interação entre humano e máquina.

Existem keyloggers baseados em hardware e em software, este último é o mais comum, dado sua facilidade e baixo custo de criação, esta modalidade terá o foco deste trabalho. Estes keyloggers precisam ser adaptados para cada sistema operacional que deseja atacar, para assegurar que a entrada e saída seja manuseada apropriadamente. Diferenças entre sistemas acarretam mecanismos específicos implementados em keyloggers de software: uso de tabela de estado do teclado, ganchos de rotina do sistema, e drivers de camadas de kernel (TULI, 2013).

2.5 Formas de ataque e prevenção

Malwares evoluem frequentemente, assim como as formas de disseminação dos mesmos. A forma mais comum de ataque é por meio dos cavalos de tróia, softwares ou arquivos que possuem malwares ocultos em seu conteúdo.

Formas de prevenção contra estes ataques crescem acompanhando a evolução dos malwares, buscando blindar os dados e informações dos usuários dos ataques causados por ferramentas maliciosas.

Proteção contra malware baseado em rede para impedir acesso não autorizado, atualizações contínuas e em tempo hábil para proteger o usuário contra ameaças, serviço de prevenção contra intrusão (IPS) e utilizar um antivírus no PC dos usuários em conjunto com firewalls corporativos são algumas das formas de prevenção conhecidas (CAMPELO, 2016).

2.6 Ferramentas Utilizadas

Nessa seção, destacamos as ferramentas necessárias a implementação desse trabalho.

- Microsoft Windows: Plataforma de execução
- MinGW: Ferramenta de compilação
- Sublime Text: Editor de texto.
- Linguagem C++: Linguagem de programação
- Ardamax: Ferramenta de criação de keylogger.

3 Metodologia

O processo de desenvolvimento do keylogger, foi em primeiro momento implementado com a ferramenta Ardamax, onde por meio dela foi entendido os conceitos e funcionalidades de uma aplicação desse tipo. Essa etapa foi importante na aquisição de conhecimento, entretanto foi decidido a não continuação dessa forma de implementação, pois a ferramenta Ardamax se trata de uma aplicação proprietária, onde suas funcionalidades são limitadas para uso gratuito.

Finalmente, os membros da equipe optaram na construção da aplicação utilizando a linguagem C++, onde os conhecimentos adquiridos são mais concretos e as funcionalidades atingidas podem seguir melhor aos requisitos do projeto.

4 Conclusões

Os resultados obtidos neste trabalho foram listados na tabela 1, onde é possível verificar os requisitos atingidos no planejamento do projeto, como também os que não foram alcançados.

Requisitos	Estado
Coletar as Teclas Digitadas pelo Usuário	Concluído
Esconder a execução do keylogger do Usuário	Concluído
Informar qual processo está em execução no momento que o usuário estiver digitando	Concluído
Funcionar em diferentes versões do Windows	Concluído
Converter o arquivo executável gerado, em um arquivo de imagem	Inicial
Executar durante a inicialização do Windows	Inicial
Enviar os dados coletados na máquina da vítima, para o email do atacante	Inicial

Tabela 1: Requisitos do Projeto

Referências

ALECRIM, Emerson **Malwares: o que são e como agem**. Disponível em:<http://www.infowester.com/malwares.php> Acessado em 29 de novembro de 2016.

CAMPELO, E. (2016) *Por que a Alerta security?* Available at: http://www.alertasecurity.com.br/blog/38-como-se-prevenir-contra-ciberataques (Accessed: 1 December 2016).

Cyber-attack (2016) in *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Cyber-attack (Accessed: 28 November 2016).

PELTIER, Thomas R. **Information Security Fundamentals, Second Edition.** United States: Taylor & Francis Group, 2013.

TULI, Preeti; SAHU, Priyanka. **System Monitoring and Security Using Keylogger.** 2013.