Universidade Federal do Rio de JANEIRO
Aluno: Jefferson Maxwell de Oliveira Ferreira
Projeto: Gris- Grupo de Resposta a Incidentes de segurança
Assunto: Criando um Malware

Bem, Eu criei um simples KeyLogger silencioso em python, como não tenho muito conhecimento no assunto decidi fazer uma coisa mais simples e rodavél. No meu projeto foi adicionado quatro arquivos : Um é o arquivo Keylogger em liguagem python, um arquivo .bat, um arquivo gbs e um arquivo de atalho do arquivo gbs para funcionar como bait.

Primeiramente, vou comentar sobre o arquivo em Python que é o algoritmo do malware que utiliza em especial a biblioteca ‘pynput’ que sem ele não teria como relizar os comandos; e foram importados logging, Key e Listener assim resumindo a linha “def on_press(key):” é responsável por capturar as teclas pressionadas e a linha “with Listener(on_press=on_press) as listener:” como capaz de escutar a tecla; desse modo, conseguimos começar a obter todas as teclas do teclado.
Porém, para tornar o código silencioso precisamos de um artifício para não precisar abrir o cdm e acionar o comando então com ajuda do arquivo teste.bat que contém informações que redirecionarão a pessoa que clicar no arquivo para uma página qualquer, que no caso foi o site facebook, e no mesmo momento o programa vai mudar para a pasta atual e abrir a pasta cdm que não resolve o nosso problema de 'Stealth' e por isso que utilizaremos o último arquivo que é o segundoplano.gbs que criará um objeto shell que chamará o CMD no modo silencioso representado por - objSh.Run"cmd/k.teste.bat",0 - que vai abrir o malware no modo silencioso,porém quem vai clicar em um arquivo estranho do nada então, com um jeito de deixar mais camuflado eu criei um arquivo de atalho de segundoplano.gbs que eu alterei o nome e a imagem do ícone através de propriedades que ajudará a manter o programa rodando sem a pessoa ter percebido que o Keylogger está rodando em segundo plano com o navegador.

E para terminar o programa de vez, terá que nas configurações do computador e depois ir no gerenciador de tarefas do windows, encontrar programa python (32 bits) assim clicar para abrir as opções e finalizar o programa e dar um fim à captura de movimentação do teclado. E será criado um arquivo texto chamado ‘Key_log.txt’ que será registrado todos os comandos ordenados pelo teclado durante a execução do programa.