Nomes: Andre Mendes , jose Eduardo, Gean
etapa 1:

Linguagem: phyton
etapa 2:
Criptografa quando executada.
Ao ser executado, encontra os arquivos de dados do usuário em sua pasta, criptografa e exclui os dados de arquivo.
Os arquivos serão zipados,dentro do malware há o zip pronto para execução, garantindo que será possível a conversão para zip.
Apagar (exemplo: usando dd) arquivos.
Limitação de dados apagados e criptografados por minuto, para não gerar suspeitas.
Ambiente alvo: linux
Alvo do malware: dados do usuário que rodou a biblioteca
Alvo de ataque: Usuários de bibliotecas de software.
etapa 3:
https://github.com/CYBERDEVILZ/Cryptonite

pedir resgate dos dados.
Exibir conta em bitcoin na tela do usuário para depósito do dinheiro.
Exibir ao usuário que caso ele não efetue o pagamento dentro de 12 horas, os dados serão apagados.
Objetivo: Ganhar dinheiro

Mo

definição do alvo
pessoas que queiram descompactar arquivo em zip no windows 10

objetivo final
entrar criptografar apagar e pedir o resgate

tecnologias usadas
python
7zip
virtual box
github
baixiaki

se der bom
se for feito o pagamento será enviado um email com a chave para desbloquear
email cadastrado no windows

se der ruim
terá um temporizador de 12 horas que se caso o usuário não fizer o pagamento será……

https://learn.microsoft.com/pt-br/windows/msix/packaging-tool/know-your-installer
https://packaging.python.org/pt_BR/latest/guides/packaging-binary-extensions/
https://msixhero.net/get/
https://github.com/CYBERDEVILZ/Cryptonite
https://github.com/TiagoAssuncao/cria-binario-exe-python
https://gist.github.com/marcoscastro/5a2053fddae87aff4401