PYVIL – NOVO TROJAN BASEADO EM PYTHON

Douglas Deobald[1]
Anderson santos da silva[2]
Roberto Bartzen Acosta[3]
Maicon dos Santos [4]

RESUMO

O PyVil, um código malicioso é ferramenta de um grupo conhecido como Evilnum, através de uma operação de hacking este malware trojan recentemente foi desenvolvido em uma ação que visa organizações de tecnologia financeira, e tem como objetivo de roubar senhas, endereços de e-mail, informações confidenciais corporativas entre outros.
Palavras-chave: PyVil, trojan, Evilnum.

ABSTRACT

PyVil, a malicious code is the tool of a group known as Evilnum, through a hacking operation this malware trojan was recently developed in an action aimed at financial technology organizations, and aims to steal passwords, email addresses , corporate confidential information and more.
Keywords: PyVil, trojan, Evilnum.

[1]Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. douglas.deobald@alcidesmaya.edu.br
[2]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. Anderson_silva@alcidesmaya.edu.br
[3]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. roberto_acosta@alcidesmaya.edu.br
[4]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. maicon_santos@alcidesmaya.edu.br

O grupo Evilnum, tem como alvos empresas de tecnologia financeira, e criou uma nova ferramenta, um trojan de acesso remoto (remote trojan acess, RAT) baseado em Python, apelidado de PyVil.

Segunado a Cybereason, conceituada empresa de tecnologia e segurança, o PyVil RAT permite que os invasores extraiam dados, façam capturas de tela e executem keylogging (gravar as teclas pressionadas no teclado), também podem implementar ferramentas de coleta de credenciais secundárias, como LaZagne (aplicativo usado para recuperar senhas armazenadas em um computador). Os ataques começam por meio de e-mails de phishing, estes então fornecem arquivos compactados com arquivos LNK fingindo ser cartões de crédito, carteiras de motorista, contas de luz e outros arquivos confidenciais, os documentos utilizados são geralmente roubados e pertencem a pessoas reais.

Este trojan é compilado com py2exe, que converte scripts python em executáveis do Windows, sendo assim, isto permite que ele baixe novos módulos para expandir sua funcionalidade. É configurado de forma que possa conter instruções para o navegador ao se comunicar com o servidor de Comando e Controle (CC). As comunicações CC são feitas por meio de solicitações, através do método de requisição POST que é suportado pelo protocolo HTTP e são criptografadas por RC4 (algoritmo simétrico de criptografia), usando uma chave codificada permanentemente, codificada com Base64 (converte os dados binários em formato de texto), assim então ele enviará informações do usuário e do sistema antes de aguardar outros comandos.

REFERÊNCIAS

https://olhardigital.com.br/fique_seguro/noticia/fintechs-sao-alvo-de-novo-malware-escrito-em-python/106504. Acesso em 24 de outubro de 2020.

https://www.enigmasoftware.com/pt/novo-pyvil-rat-ameaca-persistente-avancada-aparece-arsenal-malware-evilnum/ Acesso em: 23 outubro 2020.

https://securityaffairs.co/wordpress/107890/apt/evilnum-apt-pyvil-rat.html. Acesso em: 24 outubro 2020.