# O backdoor ChillyHell retorna para ameaçar os sistemas macOS. - Against

Data: 2025-09-15 07:31:26

Autor: Inteligência Against Invaders

Redazione RHC**:15 setembro 2025 07:39**

Pesquisadores denunciei um novo aumento na atividade para **Inferno Frio**, um backdoor modular para macOS que se pensava estar inativo há anos, mas que *parece ter infectado computadores sem ser detectado por anos*. Uma amostra do malware foi descoberta em maio de 2025 no VirusTotal, embora vestígios de sua atividade remontem pelo menos a 2021.

O ChillyHell é escrito em C++ e tem como alvo as arquiteturas Intel. Foi estudado pela primeira vez por membros da equipe Mandiant em 2023, quando eles vincularam o backdoor ao **UNC4487** grupo. A equipe hackeou um site de seguro de carro ucraniano usado por funcionários do governo para reservar viagens. Apesar da publicação da Mandiant, a amostra em si não foi sinalizada como maliciosa na época, permitindo que continuasse se espalhando sem ser detectada pelo software antivírus.

O mais alarmante é que **a cópia descoberta foi assinada pelo desenvolvedor e foi autenticada pela Apple em 2021**. *Pesquisadores do Jamf Threat Labs, Ferdous Saljuki e Maggie ZirnheltObservou* que a funcionalidade da versão corresponde quase completamente ao exemplo descrito anteriormente. Ao mesmo tempo, o arquivo **está disponível gratuitamente na pasta pública do Dropbox há quatro anos** e pode infectar sistemas enquanto permanece na categoria confiável.

Não se sabe o quão difundido foi o ChillyHell. De acordo com Jaron Bradley, chefe do Jamf Threat Labs, é **“impossível dizer” quantos sistemas foram afetados.** Com base na arquitetura do backdoor, os analistas tendem a acreditar que ele foi criado por um grupo de cibercriminosos e usado em ataques mais direcionados, em vez de em massa. A Apple já revogou os certificados dos desenvolvedores associados ao ChillyHell.

O backdoor tem três mecanismos para persistência do sistema. Se o programa for iniciado com privilégios de usuário, ele se registrará como **Agente de lançamento**; com privilégios elevados, ele se registra como **Daemon de lançamento**. Além disso, um método de backup é usado: *modificando os arquivos de configuração do shell do usuário (.zshrc, .bash_profile ou .profile), que incorporam o comando autorun, que aciona o ChillyHell para ser ativado a cada nova sessão de terminal.*

Para permanecer invisível, ele usa uma tática rara do macOS chamada **Tomada de tempo**, em que arquivos maliciosos *são atribuídos carimbos de data/hora que correspondem a objetos legítimos para evitar serem notados.* O ChillyHell também alterna entre protocolos de comando e controle, tornando a detecção muito mais difícil.

A arquitetura modular permite que invasores *para expandir a funcionalidade de forma flexível após a implantação.* O backdoor pode baixar novas versões do próprio se, instalar componentes adicionais, realizar ataques de força bruta, salvar nomes de usuário locais para futuras tentativas de hacking e iniciar o roubo de credenciais. Essa combinação o torna uma plataforma conveniente para novos ataques e presença de longo prazo no sistema.

Os pesquisadores enfatizam que a combinação de mecanismos de persistência, a variedade de protocolos de comunicação e o design modular tornam o ChillyHell uma ferramenta extremamente flexível. Eles também observam que ele foi submetido ao processo de autenticação da Apple, demonstrando que o malware nem sempre é assinado digitalmente.

**Redação**
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli