Ataque Terrapin

Caio Abreu Ferreira

Análise técnica do Ataque Terrapin

29 de janeiro de 2024

Resumo Executivo

O ataque cibernético denominado Terrapin representa uma ameaça significativa, visando o protocolo SSH amplamente empregado por administradores de sistemas para acesso remoto. A exposição desse protocolo ressalta a necessidade crítica de medidas preventivas e de mitigação. Dada a larga utilização do protocolo SSH na infraestrutura de TI, a proteção contra o Terrapin torna-se necessário. A consciência e a ação proativa diante dessa ameaça são essenciais para preservar a estabilidade e a segurança.

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

Sumário

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

1 Introdução

O Ataque Terrapin representa uma ameaça significativa ao protocolo criptográfico SSH. O protocolo SSH é amplamente empregado por administradores de sistemas para acessar servidores remotamente. Este ataque compromete a segurança do SSH ao realizar um downgrade por meio de uma interceptação man-in-the-middle. O presente texto constitui uma análise técnica detalhada desse ataque.

2 Protocolo SSH

2.1 O que é

Desenvolvido com o propósito de substituir protocolos não criptografados, como Telnet e RSH, e protocolos de transferência de arquivos desprotegidos, como FTP e RCP, o SSH estabelece conexões seguras e criptografadas entre dois dispositivos. Os administradores empregam predominantemente o protocolo SSH para realizar logins remotos, acessar máquinas em suas redes, efetuar transferências de arquivos, executar comandos e administrar aplicações.

2.2 Como funciona

O funcionamento do protocolo segue o modelo cliente-servidor, em que a conexão é iniciada pelo cliente SSH, estabelecendo conexão com o servidor SSH. O cliente SSH inicializa o processo de estabelecimento da conexão, utilizando criptografia do tipo chave pública-privada para autenticar o servidor SSH. Após a fase de configuração, o protocolo SSH utiliza criptografia do tipo simétrica e algoritmos de hashing para assegurar a privacidade

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

e integridade dos dados trocados entre cliente e servidor.

A Figura 1 apresenta um fluxo de configuração simplificado de uma conexão shell segura.

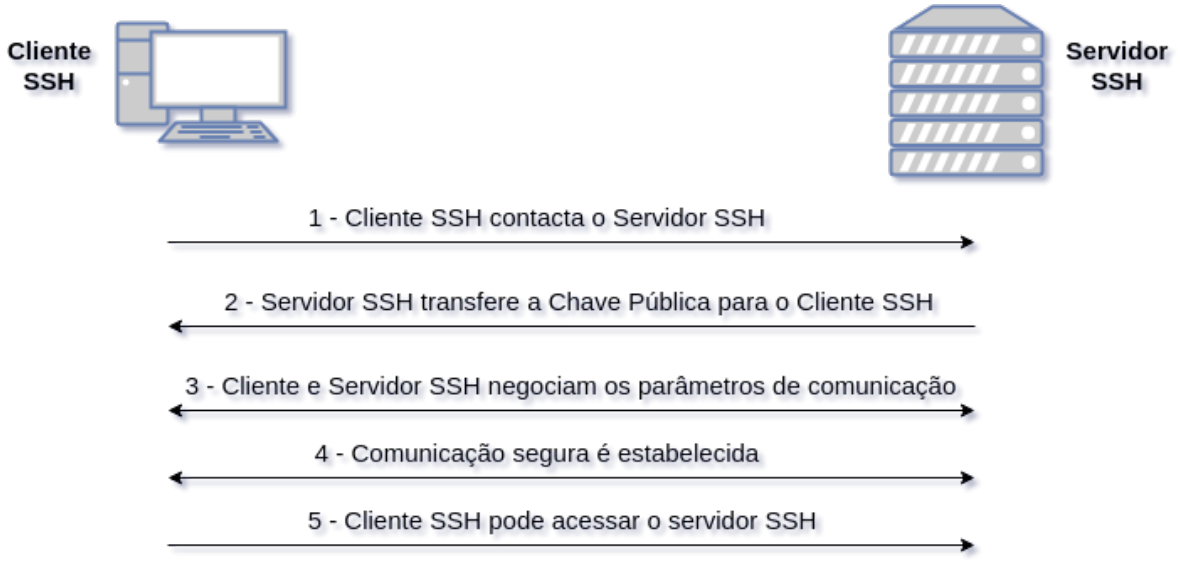

Figura 1: Descrição do funcionamento do protocolo SSH

1. Por meio de um software gráfico ou utilizando a linha de comando, o Cliente SSH estabelece a comunicação inicial com o Servidor SSH por meio do protocolo TCP;
2. O servidor SSH transmite a Chave Pública utilizando o algoritmo de criptografia RSA assimétrico;
3. O Servidor SSH e o Cliente SSH trocam informações relativos ao protocolo de criptografia e outras informações pertinentes durante a comunicação;
4. Após a confirmação e estabelecimento da comunicação entre as partes envolvidas, ambas utilizam o que é conhecido

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

como Chave de Algoritmo de Troca Diffie-Hellman para gerar uma chave simétrica. Esse algoritmo possibilita que tanto o Cliente quanto o Servidor compartilhem uma chave criptografada do tipo simétrica, algoritmo de criptografia AES 256, a qual será empregada para conduzir a sessão de comunicação;

5. Este é o último estágio antes de o usuário obter suas credenciais de acesso ao servidor de forma autenticada. Nesse sentido, os usuários de SSH utilizam uma senha como meio de autenticação.

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

3 Terrapin

3.1 Descrição

O Terrapin é um tipo de ataque direcionado ao protocolo SSH que compromete a integridade do canal seguro. Especificamente, esse ataque manipula os números de sequência durante o processo de handshake, permitindo que um invasor elimine mensagens enviadas pelo cliente ou servidor no início do canal seguro sem detecção.

Este tipo de ataque pode ser executado na prática, resultando na diminuição da segurança da conexão ao truncar a mensagem de negociação de extensão da transcrição. Isso pode levar à adoção de algoritmos de autenticação menos seguros pelo cliente e à desativação de contramedidas específicas contra ataques de temporização de pressionamento de tecla no OpenSSH 9.5.

O Terrapin também pode ser explorado para aproveitar falhas na implementação do protocolo SSH, possibilitando ataques de phishing e concedendo ao invasor recursos de Man-in-the-Middle (MitM) dentro da sessão criptografada.

Para realizar o ataque Terrapin, é necessário ter recursos MitM na camada de rede para interceptar e modificar o tráfego da conexão. Além disso, a conexão deve ser protegida pelos algoritmos de criptografia **ChaCha20-Poly1305** ou **CBC com Encrypt-then-MAC**"para permitir o ataque.

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

3.2 Mitigação

Para mitigar o ataque Terrapin em um servidor ou cliente do tipo OpenSSH, é imperativo que o administrador de sistemas modifique os arquivos de configuração do OpenSSH, o arquivo **ssh_config** para o cliente e o arquivo **sshd_config** para o servidor e altere os arquivos para que fiquem igual as linhas abaixo.

- **Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr**
- **MACs hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com**

O comando acima irá remover o algoritmo de criptografia **ChaCha20-Poly1305** e o algoritmo de MAC **-etm@openssh.com** do processo de autenticação.

Na Figura 2, a ferramenta nmap está sendo utilizada para obter informações do servidor OpenSSH. Como é possível verificar no destaque da figura, o algoritmo de criptografia **ChaCha20-Poly1305** e o algoritmo de MAC **-etm@openssh.com** não estão sendo utilizados.

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

```
cferreira@debian ~ nmap --script ssh2-enum-algos -sV -p 59022 192.168.122.30
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-29 14:57 -03
Nmap scan report for 192.168.122.30
Host is up (0.00066s latency).

PORT      STATE SERVICE VERSION
59022/tcp open  ssh     OpenSSH 8.4p1 (protocol 2.0)
| ssh2-enum-algos:
|   kex_algorithms: (5)
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp521
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp256
|       diffie-hellman-group-exchange-sha256
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (5)
|       aes256-gcm@openssh.com
|       aes128-gcm@openssh.com
|       aes256-ctr
|       aes192-ctr
|       aes128-ctr
|   mac_algorithms: (3)
|       hmac-sha2-512
|       hmac-sha2-256
|       umac-128@openssh.com
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
```

Figura 2: Ferramenta nmap utilizada para verificar o servidor OpenSSH

Nas demais implementações do protocolo SSH, recomenda-se avaliar a eventual necessidade de modificar o arquivo de configuração ou realizar a atualização do software correspondente.

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

Copyright
Este documento está licenciado sobre a licença Creative Commons BY-NC-SA

Propósito deste documento
Ataque Terrapin - Análise técnica do Ataque Terrapin

Versão
Versão 2024.01

Autor
Caio Abreu Ferreira [abreuferr@gmail.com]

Este documento está licenciado sobre a licença Creative Commons BY-NC-SA