



NOxCrypt v2.3.0 — Especificação Pública

Autor: NOX

1. Nome

NOxCrypt v2.3.0 é um algoritmo criptográfico proprietário desenvolvido especificamente para o sistema NOX. Seu objetivo é fornecer uma criptografia que não possa ser reconhecida como tal, inclusive disfarçada como formatos de mídia diversos e fluxos binários aleatórios. Também é baseado no mecanismo Deep InCryption (desenvolvimento da NOX).

2. Objetivos e Características

- Ocultar não apenas o conteúdo dos dados, mas também o fato de sua existência.
- Os dados de saída podem imitar imagens, áudio, vídeo ou dados binários arbitrários.
- Disfarçar como formatos populares (ex.: JPEG, MP3, PNG).
- Uso exclusivo dentro do ecossistema NOX.
- Chave dinâmica, gerada de forma única para cada sessão.
- Mecanismo Deep InCryption (desenvolvimento da NOX) como camada adicional de privacidade.

3. Arquitetura

A arquitetura utiliza estágios em cascata de transformação de dados, incluindo substituições, mistura e adição de ruído controlado. Esquemas matemáticos específicos e tabelas internas são informações confidenciais e não são divulgados na versão pública desta especificação.

4. Chave e Sessões

A chave de criptografia possui grande comprimento e é formada dinamicamente usando parâmetros aleatórios e de sessão. Para cada sessão são criadas tabelas e

regras de transformação únicas, impedindo a reutilização de chaves e padrões de criptografia.

5. Mascaramento

O algoritmo é capaz de converter o fluxo criptografado em uma forma correspondente a diferentes tipos de arquivos de mídia ou tráfego de rede, o que dificulta significativamente a identificação da transmissão de dados criptografados.

6. Segurança

Cada sessão utiliza chaves únicas e conjuntos próprios de regras de criptografia. Mesmo que o tráfego seja interceptado, sem acesso à chave a descryptografia é impossível. O algoritmo inclui mecanismos para prevenir a criptoanálise e mascarar a estrutura dos dados.

7. Aplicação

NOXCrypt pode criptografar texto, dados de voz e fluxos binários arbitrários, transformando-os em formas que não levantem suspeitas. O algoritmo é otimizado para alta velocidade e baixa latência durante a transmissão de dados.

8. Conclusão

NOXCrypt é um sistema criptográfico de próxima geração voltado para garantir máxima confidencialidade e anonimato, bem como resistência à detecção e análise. Esta especificação oferece uma visão geral da tecnologia e não revela os detalhes internos do algoritmo.