Ferramenta Para Monitoramento de Redes P2P - EspiaMule

PCF Guilherme Martini Dalpian
PCF Carlos Augustus Armelin Benites

Introdução

Desafios e características inerentes às redes P2P e possibilidades de monitoramento

Intenso uso dessas redes para fins ilícitos (pedofilia, direitos autorais)

Ferramenta para monitoramento das redes eDonkey e Kad utilizadas pelo eMule

ICCyber 2007
IV Conferência Internacional de Perícias em Crimes Cibernéticos

PCF Guilherme Martini Dalpian
PCF Carlos Augustus Armelin Benites

Roteiro

- Redes ponto-a-ponto (P2P)
- O aplicativo eMule
  - Identificação dos Arquivos (Links ED2K)
  - Identificação dos Clientes
  - Autoria e Materialidade
- EspiaMule
- Próximos Passos
- Conclusão

Redes ponto-a-ponto (P2P)

- Independência de servidores centrais
- Rede eDonkey
- Rede Kad
- Outras redes (bittorrent, gnutella, kazaa)

O aplicativo eMule

- Utiliza as redes eDonkey e Kad (independentes)
- Estimativa: 5 a 20 milhões de usuários simultâneos
- Compartilhamento obrigatório de arquivos baixados
- Identificação única de usuários (hash de usuário)
- Buscas por palavras-chave

Identificação dos Arquivos (Links ED2K)

- Identificação de arquivos a partir de hash MD4 (independente do nome do arquivo)
- Garante a integridade e identificação do arquivo baixado
- Como é um link, pode ser redistribuído

Identificação dos Clientes

- Identificados a partir do hash de usuário
- Busca de arquivos por palavras-chave
- Busca de fontes disponíveis para links ED2K
- ID-Alta e ID-Baixa
- Não suporta conexões ID-Baixa com ID-Baixa

Autoria e Materialidade

- Ao se buscar arquivo a partir de link ED2K, há garantia de que as fontes possuem o arquivo (ou parte dele)
- Identificação dos clientes a partir do endereço IP e hash do usuário
  - Redes privadas
  - Trojans/proxies
  - Hash de usuário clonado

EspiaMule

- Aplicativo eMule modificado a partir do código fonte, disponível na web
- Armazena IP, data e hora de todos os clientes compartilhando os arquivos baixados
- Bloqueio total de upload
- Forma de uso:
  - Idêntico ao aplicativo eMule disponível na rede
  - Permite buscas nas redes Kad e eDonkey
  - Permite buscas por palavras-chave ou download a partir de links ED2K

EspiaMule

- Processamento do log:
  - Aplicativo em java
  - Identifica os usuários pelo país
  - Separa automaticamente usuários por provedor através de pesquisas WHOIS
  - Pode agrupar clientes com diversos arquivos a partir do hash de usuário ou IP

EspiaMule

- Cuidados:
  - Hashes de usuários suscetíveis de clonagem
  - Dificuldade de autoria: IP pode ser compartilhado ou "roubado"
  - Arquivos parciais
- Sugestão (para o caso de pedofilia):
  - Focar em usuários com vários arquivos compartilhados (ex.: 5 ou mais arquivos)

Conclusão

- Aplicativo disponível para uso interno do Departamento de Polícia Federal
- Novos rumos:
  - Atualizações de versão do eMule
  - Novas redes: bittorrent, gnutella, etc.
- Dúvidas:
  - dalpian.gmd@dpf.gov.br
  - benites.caab@dpf.gov.br