Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers

Jean Massucatto[1]
Matheus Kowalczuk Ferst[1]

[1]Departamento Acadêmico de Informática
Universidade Tecnológica Federal do Paraná

Sumário

Introdução

- Todos os dias milhares de domínios são abandonados por seus donos e se tornam disponíveis para serem re-registrados.
- Para domínios `.com` esse valor chega a 75k/dia.
- 10% de todos os domínios `.com` são re-registrados no mesmo dia.
- O valor chega a 50% para domínios `.org`, com um tempo médio de 30s para ser re-registrado.
- Essa concorrência acirrada existe devido a especulação de domínios, em especial por parte de serviços de *drop-catch*.

Introdução

- Todos os dias milhares de domínios são abandonados por seus donos e se tornam disponíveis para serem re-registrados.
- Para domínios `.com` esse valor chega a 75k/dia.
- 10% de todos os domínios `.com` são re-registrados no mesmo dia.
- O valor chega a 50% para domínios `.org`, com um tempo médio de 30s para ser re-registrado.
- Essa concorrência acirrada existe devido a especulação de domínios, em especial por parte de serviços de *drop-catch*.

Introdução

- Todos os dias milhares de domínios são abandonados por seus donos e se tornam disponíveis para serem re-registrados.
- Para domínios `.com` esse valor chega a 75k/dia.
- 10% de todos os domínios `.com` são re-registrados no mesmo dia.
- O valor chega a 50% para domínios `.org`, com um tempo médio de 30s para ser re-registrado.
- Essa concorrência acirrada existe devido a especulação de domínios, em especial por parte de serviços de *drop-catch*.

Introdução

- Todos os dias milhares de domínios são abandonados por seus donos e se tornam disponíveis para serem re-registrados.
- Para domínios `.com` esse valor chega a 75k/dia.
- 10% de todos os domínios `.com` são re-registrados no mesmo dia.
- O valor chega a 50% para domínios `.org`, com um tempo médio de 30s para ser re-registrado.
- Essa concorrência acirrada existe devido a especulação de domínios, em especial por parte de serviços de *drop-catch*.

Introdução

- Todos os dias milhares de domínios são abandonados por seus donos e se tornam disponíveis para serem re-registrados.
- Para domínios `.com` esse valor chega a 75k/dia.
- 10% de todos os domínios `.com` são re-registrados no mesmo dia.
- O valor chega a 50% para domínios `.org`, com um tempo médio de 30s para ser re-registrado.
- Essa concorrência acirrada existe devido a especulação de domínios, em especial por parte de serviços de *drop-catch*.

Introdução

- Especulação é definida como a compra de um ativo com a esperança que este valorize-se no futuro.
- Ocorre em diferentes áreas.
  - Como a especulação financeira.
    - Febre das tulipas
    - Bolha do alho-poró
  - Ou a especulação imobiliária.
- Este tipo de processo pode levar o valor do ativo a desvia-se de seu valor intrínseco.
- A especulação de domínios é a compra de um endereço que acredita-se que será requisitado em breve.

Introdução

- Especulação é definida como a compra de um ativo com a esperança que este valorize-se no futuro.
- Ocorre em diferentes áreas.
  - Como a especulação financeira.
    - Febre das tulipas
    - Bolha do alicate
  - Ou a especulação imobiliária.
    - Crise de 2007-2008.
- Este tipo de processo pode levar o valor do ativo a desvia-se de seu valor intrínseco.
- A especulação de domínios é a compra de um endereço que acredita-se que será requisitado em breve.

Introdução

- Especulação é definida como a compra de um ativo com a esperança que este valorize-se no futuro.
- Ocorre em diferentes áreas.
  - Como a especulação financeira.
    - Febre das tulipas
    - Bolha do alicate
  - Ou a especulação imobiliária.
    - Crise de 2007-2008.
- Este tipo de processo pode levar o valor do ativo a desvia-se de seu valor intrínseco.
- A especulação de domínios é a compra de um endereço que acredita-se que será requisitado em breve.

Introdução

- Especulação é definida como a compra de um ativo com a esperança que este valorize-se no futuro.
- Ocorre em diferentes áreas.
  - Como a especulação financeira.
    - Febre das tulipas
    - Bolha do alicate
  - Ou a especulação imobiliária.
    - Crise de 2007-2008.
- Este tipo de processo pode levar o valor do ativo a desvia-se de seu valor intrínseco.
- A especulação de domínios é a compra de um endereço que acredita-se que será requisitado em breve.

Introdução

- Especulação é definida como a compra de um ativo com a esperança que este valorize-se no futuro.
- Ocorre em diferentes áreas.
  - Como a especulação financeira.
    - Febre das tulipas
    - Bolha do alicate
  - Ou a especulação imobiliária.
    - Crise de 2007-2008.
- Este tipo de processo pode levar o valor do ativo a desvia-se de seu valor intrínseco.
- A especulação de domínios é a compra de um endereço que acredita-se que será requisitado em breve.

Introdução

- Especulação é definida como a compra de um ativo com a esperança que este valorize-se no futuro.
- Ocorre em diferentes áreas.
  - Como a especulação financeira.
    - Febre das tulipas
    - Bolha do alicate
  - Ou a especulação imobiliária.
    - Crise de 2007-2008.
- Este tipo de processo pode levar o valor do ativo a desvia-se de seu valor intrínseco.
- A especulação de domínios é a compra de um endereço que acredita-se que será requisitado em breve.

Introdução

- Especulação é definida como a compra de um ativo com a esperança que este valorize-se no futuro.
- Ocorre em diferentes áreas.
  - Como a especulação financeira.
    - Febre das tulipas
    - Bolha do alicate
  - Ou a especulação imobiliária.
    - Crise de 2007-2008.
- Este tipo de processo pode levar o valor do ativo a desvia-se de seu valor intrínseco.
- A especulação de domínios é a compra de um endereço que acredita-se que será requisitado em breve.

Introdução

- Quando um domínio é registrado por especulação, geralmente coloca-se uma página informado que o domínio está a venda.
- Este tipo de página é chamada de *parking page*, e geralmente contém inúmeras propagandas, a fim de monetizar minimamente e gerar algum retorno do investimento no domínio mesmo antes de sua venda.
- Um fenômeno observados nos anos anteriores a 2008 e 2009 foi a "Degustação de domínios", onde um domínio era registrado apenas para observar o tráfego, e apagado antes do fim do *Add Grace Period* (AGP).

Introdução

- A ICANN (*Internet Corporation for Assigned Names and Numbers*) tomou medidas para diminuir esta prática, considerada abusiva.
- Hoje o número de reembolsos por cancelamento de domínios durante o AGP é limitado a 50 reembolsos ou 10% do tráfego do registrador de domínios, o que for maior.
- Esta medida fez com que a prática diminuísse drasticamente após 2009.

Introdução

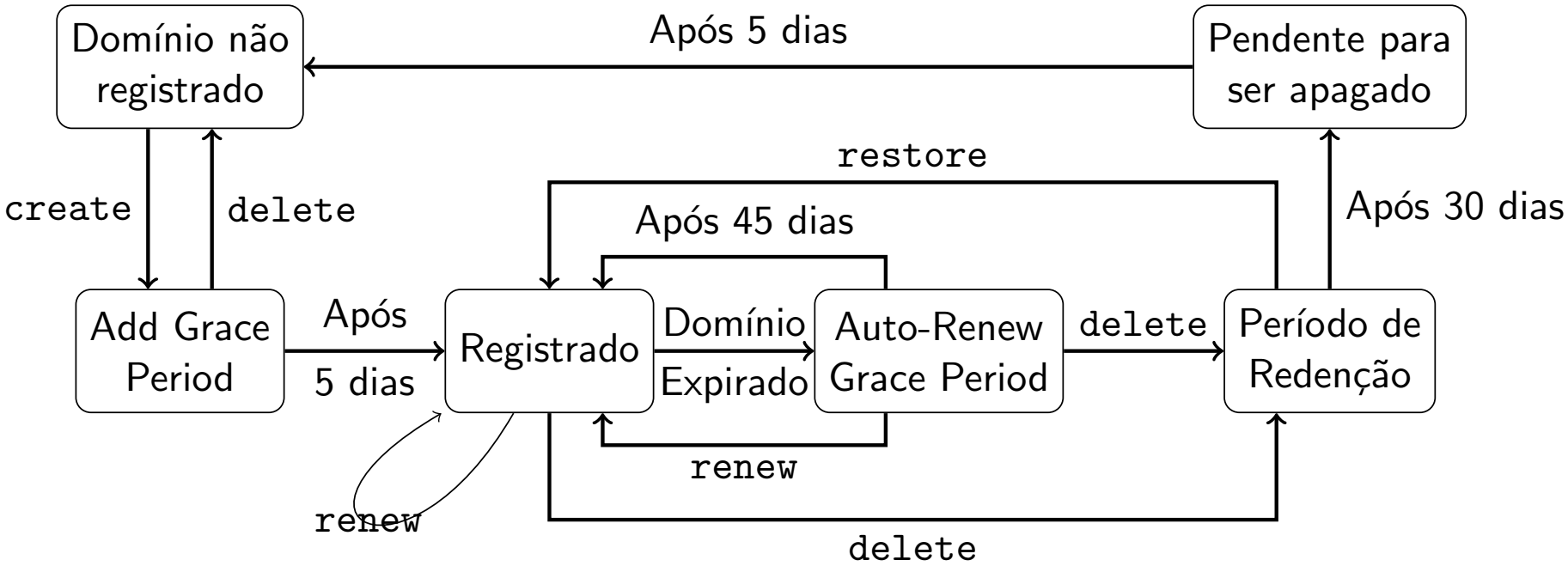

Figura: Processo de registro de um domínio

Introdução

- O re-registro de domínios também pode assumir caráter malicioso.
  - Envio de spam.
  - *Typosquatting*.
  - Um domínio que antes hospedava o JavaScript para outras páginas e foi desativado pode ser re-registrado para injetar códigos maliciosos nestas páginas.
  - Cookies podem ser obtidos de uma página que deixou de existir.
  - etc.
- O foco do artigo entretanto não é na motivação para um domínio ser re-registrado, mas sim na quantificação do processo de re-registro.

Introdução

- O artigo identifica quatro cenários que levam o registro de um domínio a mudar de dono:
  - Venda direta: o dono de um domínio pode passar a propriedade deste para outra pessoa interessada no mesmo domínio.
  - Pre-release: o domínio pode ser vendido após ter expirado, mas antes de ser apagado, como durante o *Auto-Renew Grace Period*
  - Drop-catch: o domínio pode ser re-registrado imediatamente após ser apagado.
  - Convencional: o domínio pode ser re-registrado em algum momento futuro após ter sido apagado.

Introdução

- O processo convencional e de venda direta já foram estudados em outros artigos.
- O foco deste artigo está nas transferências por pre-release e drop-catch.
- O processo de pre-release tem ainda implicações de subverter o processo de re-criação do domínio, evitando que alguns metadados do domínio mudem.
    - Alguns filtros de spam, como o Predator e Spamhaus, se baseiam nestes dados para identificar domínios de spam.

Introdução

- Após expirado, o domínio pode ser re-registrado em um esquema “primeiro-a-chegar”.
- Durante certos horários que dependem da zona em que o domínio está registrado e a atual empresa que registrou o domínio, o será liberado.
- Este evento é denominado de “drop”.
- Neste momento os serviços de drop-catch buscam realizar inúmeras requisições na tentativa de conseguir o domínio.

Introdução

- O flood de requisições é tão grande que alguns autores consideram ser "o maior ataque de negação de serviços legalizado".
- O artigo mostra que cerca de 80% das tentativas de criação de domínios são de serviços de drop-catch, enquanto apenas cerca de 9.5% das requisições de registro com sucessão são oriundas deste tipo de serviço.
- Alguns serviços de drop-catch tentam se posicionar geograficamente próximos aos serviços de registro para que suas requisições cheguem primeiro.
- Estes serviços também procuram realizar engenharia reversa na forma em que os registros percorrem a lista de domínios que serão apagados para tentar prever o exato instante em que o domínio estará livre.

Introdução

- A prática de drop-cathing é controversa.
  - Alguns serviços de registro desencorajam a prática, como os domínios `.uk` que cobram por tentativas falhas de registro.
  - Outros incentivam, disponibilizando listas de domínios que estão próximos de expirar ou de serem apagados.
- O artigo considera a análise como drop-catch re-registros que ocorrem no mesmo dia em que os domínios são apagados, o "dia 0".

Introdução

- O artigo realizou um estudo durante quatro semanas em julho de 2016 analisando mais de 4 milhões de domínios.
- Outro estudo foi realizado no início de 2017 durante uma semana a fim de caracterizar alguns aspectos da degustação de domínios que não poderiam ser observados pelo método aplicada anteriormente.

Introdução

- O método aplicado consistia principalmente na consulta dos domínios em servidores de DNS e em servidores WHOIS.
- Servidores WHOIS impõem restrições na taxa de requisições que podem ser feitas, de forma que a grande quantidade de domínios observados no primeiro estudo inviabilizava um acompanhamento preciso de alguns eventos.

Introdução

- Os domínios monitorados foram obtidos de diversas listas de domínios próximos a serem apagados, disponibilizadas por alguns serviços de registro e pelos próprios serviços de drop-catch.
- Alguns esforços foram realizados para juntar estar listas, que possuíam grande sobreposição e discrepâncias de cerca de um dia entre as possíveis datas em que os domínios seriam apagados.

Introdução

- Alguns dos dados observados pelos autores:
  - Serviços de drop-catch costumam requisitar registros com duração de apenas um ano.
  - Serviços de drop-catch dificilmente mantém o registro, quase sempre a transferência do registro é imediata.
  - A nível de sucesso nas requisições de registro para serviços de drop-catch é aproximadamente 0.05%.
    - Para domínios `.com`, a taxa de falha em requisições de registro foi de 99.9% em agosto de 2016.

Introdução

- O artigo também buscou identificar clusters de IDs de registro.

Nome	IDs	%
DropCatch.com	1252	42.6 %
Pheenix.com	498	16.9 %
SnapNames.com	466	15.8 %
LogicBoxes.com	53	1.8 %
MyDomain.com	43	1.5 %
XZ.com	21	0.7 %
Name.com	19	0.6 %
Dynadot.com	19	0.6 %
22.cn	16	0.5 %
(total)	2387	81.1 %