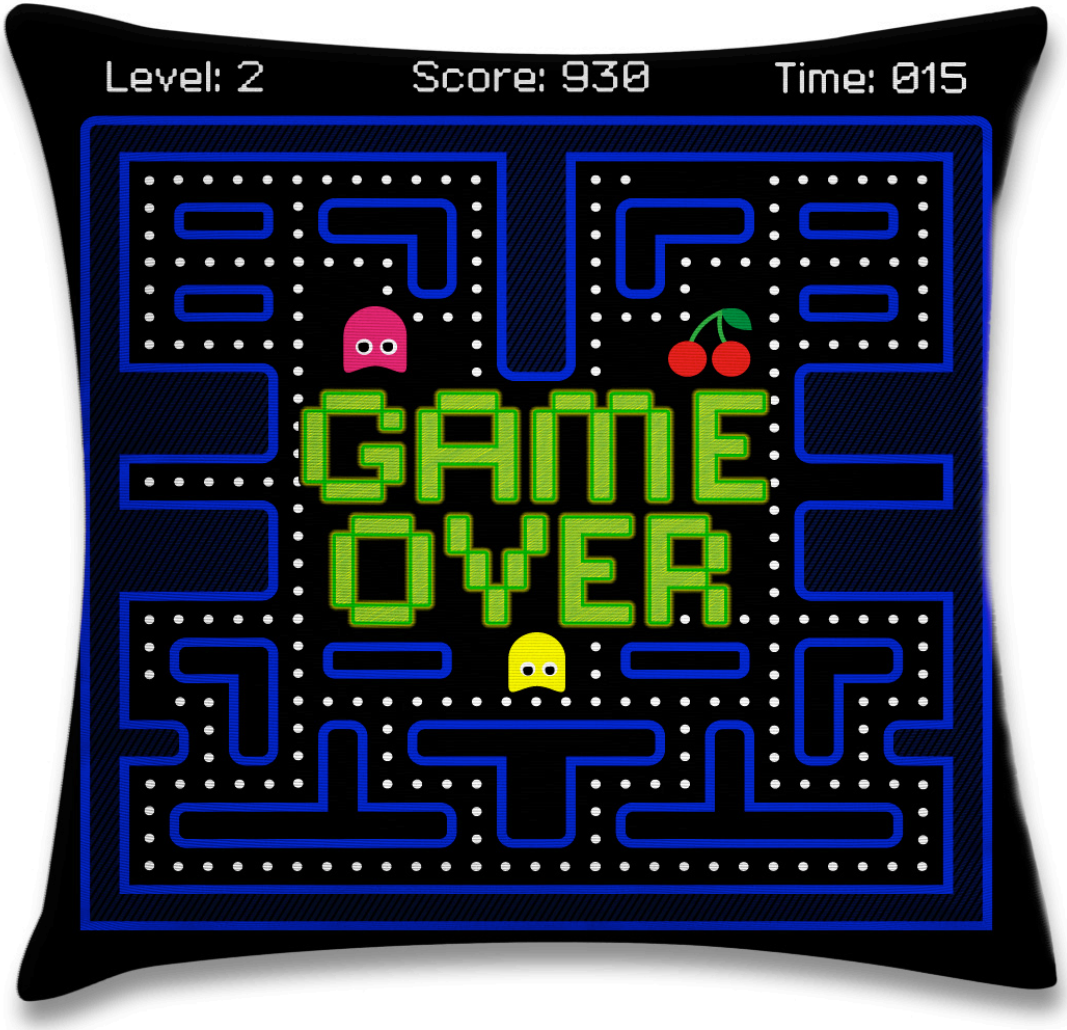
ceptro.br

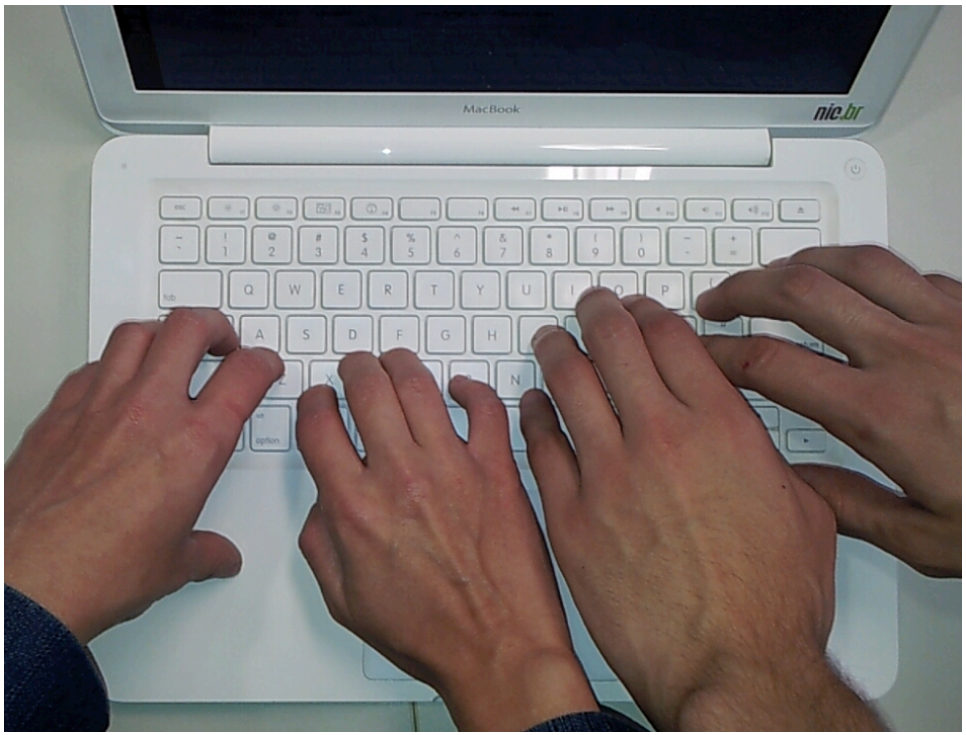
Desafios do IPv6 para profissionais de segurança

nic.br cgi.br

Caso alguém ainda não saiba, no mundo IPv4...



Desafios do NAT



- Dificuldade de identificação dos usuários
- Necessidade de alteração nos sistemas de logs
- Afeta bases de dado de reputação (blacklists)

O IPv6 existe, e está por aí...

- Diversos tipos de equipamentos têm suporte a IPv6 há décadas
- Muitos vêm com IPv6 ativo por padrão
- Alguns criam túneis automáticos para obter conectividade IPv6 (por exemplo, o Windows)
- O IPv6 não pode ser ignorado, do ponto de vista de segurança, mesmo em redes que só operam com IPv4!

Formato do endereço

- 2001:db8::1
- 2001:0DB8::1
- 2001:0Db8:0:0:0:0:0:0001
- Usar o grep para identificar um determinado IP num arquivo de log não é mais uma tarefa tão simples...
- Suas ferramentas de tratamento de logs conseguem já trabalhar com o IPv6?

Formato do endereço

- 2000::/3
  - `2000:0000:0000:0000:0000:0000:0000:0000`
    `3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`
- FC00::/7
  - `FCnn: …`
    `FDnn: …`
- FF00::/8
- ::1
- ::0/128
- ::ffff:w.x.y.z
- 2001:0db8::/32
- 64:ff9b::/96
- 2001:0000::/32
- 2002::/16

- Você já reconhece todas essas diferentes faixas de endereços?
- E seus sistemas de tratamento de logs?

Autoconfiguração e privacidade

- No IPv6 podemos ter:
  - Endereços atribuídos manualmente
  - Endereços atribuídos por DHCPv6
    - Mas nem todos os Sistemas Operacionais em uso têm suporte nativo
  - Endereços atribuídos por SLAAC
    - MACs (EUI-64)
      - Podem identificar um usuário mesmo quando ele se move entre diferentes redes
    - Aleatórios
      - Como manter a identificação do usuário numa rede corporativa?

Paridade de funcionalidades

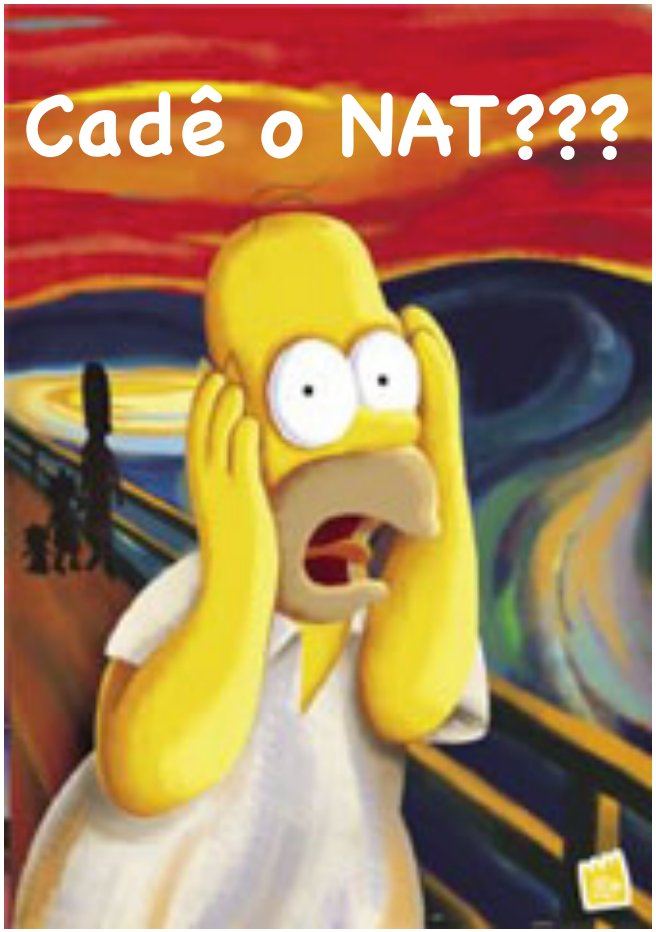
- No core da rede, o suporte ao IPv6 nos equipamentos é bastante maduro, genericamente
- Em outros tipos de equipamentos e softwares, em especial relacionados à segurança:
  - Firewalls, IDSs, SIEMs, etc
  - Nem sempre há paridade de funcionalidades, mesmo quando o fabricante afirma que o equipamento suporta IPv6. É necessário ter atenção e ser detalhista nesse ponto.

Reputação e blacklists

- É esperado que um usuário doméstico obtenha em bloco entre /64 e /56.
- Empresas trabalham geralmente com blocos /48.
- Alguns serviços de hosting oferecem um /64 ou /56 por cliente, outros oferecem múltiplos /128.
- É possível atribuir diversos endereços IPv6 simultaneamente a uma mesma interface... E há muitos, muitos mesmo, disponíveis...
- O que bloquear? Um /128? /64? Qual a granularidade ideal?
  - Há suporte já, mas deve se esperar problemas e ajustes

E meu perímetro, como fica?

- NAT66
  - Diga “Por Hoje Não!”
  - Procure um grupo de apoio
  - Use um **firewall stateful** para obter o mesmo comportamento com IPv6 que havia com IPv4 em sua rede, se isso é realmente o que você deseja!
  - Se você acredita mesmo em segurança por obscuridade, utilize endereços ULA (privados) para serviços internos que não dependem da Internet.



E o IPSEC?

- Ele está presente em praticamente todas as implementações de IPv6
  - Exceção para alguns dispositivos embarcados, com 6lowpan
- O IPSEC no IPv6 não funciona de forma mágica, sozinho
  - Da mesma forma que no IPv4 é preciso configurá-lo
- Pode ser uma ferramenta útil. Utilize-o, quando aplicável ou necessário.

Vulnerabilidades novas

- É possível utilizar **multicast** para realizar o reconhecimento numa determinada rede, descobrindo todos os hosts ativos
- Vulnerabilidades relacionadas aos **cabeçalhos de extensão** podem ser exploradas de diferentes formas:
  - Cadeias com múltiplos cabeçalhos, ou cabeçalhos mal formados, podem ser usadas em ataques de DoS
  - Informações podem ser enviadas sem que firewalls analisem o conteúdo dos pacotes

Vulnerabilidades novas

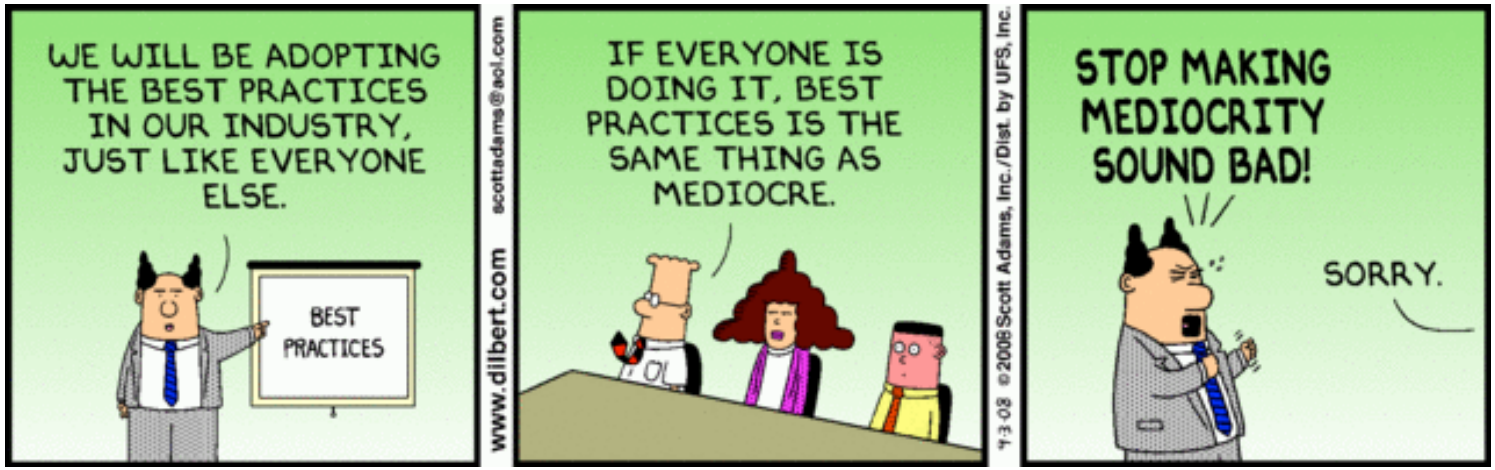
- A descoberta de vizinhança (neighbour discovery) tem algumas falhas:
  - É possível criar Router Advertisements falsos, para um ataque men in the middle, ou de negação de serviço
  - É possível congelar computadores Windows enviando RAs em grandes quantidades na rede
  - É possível falsificar respostas na descoberta de vizinhos, criando ataques do tipo men in the middle
  - É possível responder ao processo de detecção de endereços duplicados, em um ataque de negação de serviço.
- Algumas dessas falhas tem possibilidades de proteção parcial (RA Guard, por exemplo). Outras tem de ser monitoradas e tratadas.

Vulnerabilidades novas

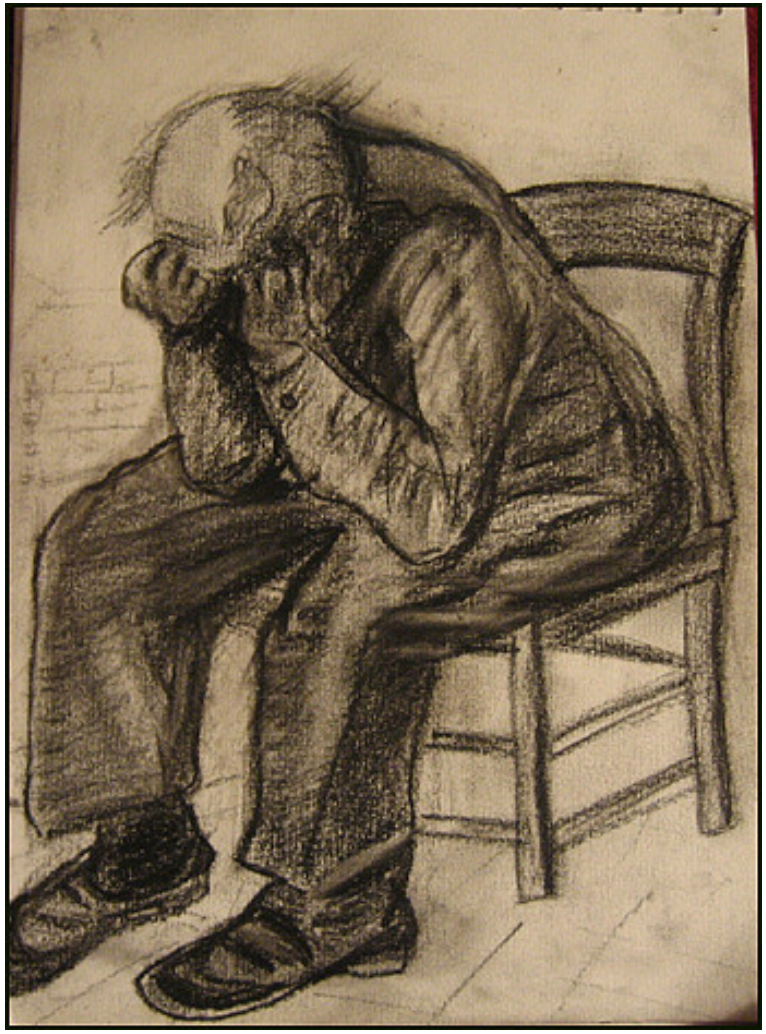
- O DHCPv6 também tem vulnerabilidades que podem ser exploradas:
  - Ao solicitar endereços em excesso a um servidor DHCPv6 stateful pode-se esgotar o bloco disponível, ou ao menos a quantidade de memória usada pelo servidor para armazenar as informações, num ataque de negação de serviço

Boas práticas, BCPs, etc...

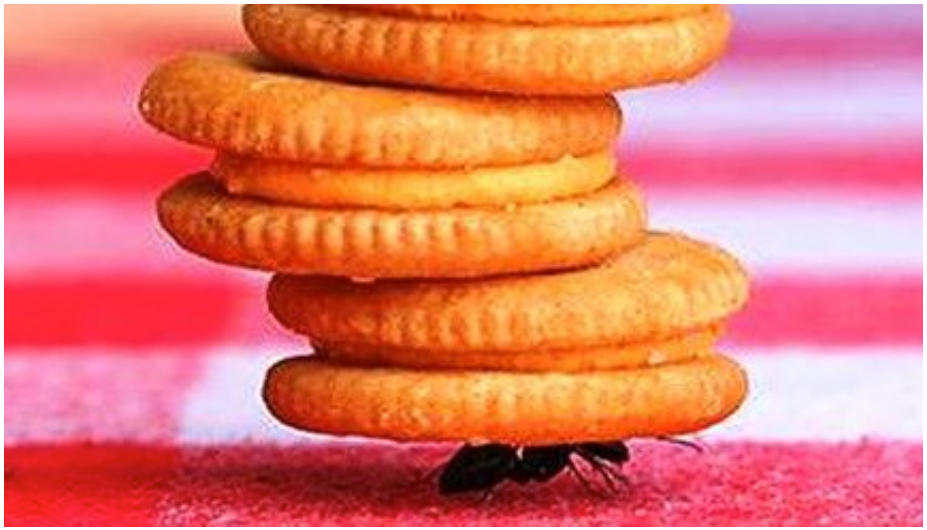
- Bom...
  - Pra haver boas práticas, é necessário haver prática, não ?
- Temos poucas para o IPv6, algumas são diferentes:
  - Como distribuir os endereços
  - Como fazer filtros, lidar com bogons



O que fazer?



Implantar o IPv6 de forma planejada



- A implantação do IPv6 é necessária e urgente
- A urgência não é a mesma para todos os elementos da rede
  - Os serviços na Internet devem ter IPv6 já
  - Dentro da rede corporativa, a urgência não é a mesma
  - Em algum momento administrar duas redes (IPv4 e IPv6) trará mais problemas do que desligar o IPv4

Dúvidas?

Antonio M. Moreiras
moreiras@nic.br