A REVISTA Nº 1 DA TECNOLOGIA

+ INVESTIGAÇÃO
+ REPORTAGEM
+ TUTORIAIS
+ TESTES

EXCLUSIVO CÂMARAS MUNICIPAIS USAM REDES VULNERÁVEIS

Nvidia Shield Tablet

Experimentámos o tablet para quem quer jogar a sério!

EXAME INFORMÁTICA

TAMBÉM EM **IPAD** E **ANDROID**

Agosto 2014 N.º 230 • Mensal • Ano 19
€3 Portugal Continental • **€5,04** Revista + DVD
www.exameinformatica.sapo.pt

LG G3
ESTÁ AQUI O MELHOR SMARTPHONE LANÇADO ESTE ANO!*

*Até agora

iOS e ANDROID *e a maioria é gratuita!*

100 APPS

DESTE ANO QUE VOCÊ NÃO CONHECE... E DEVIA!

Bq Witbox
Um preço pequeno numa máquina que imprime objetos 3D em grande!

Unbabel
A empresa portuguesa que recusou ofertas da Google e da Facebook

+

XBOX ONE
VALE A PENA? É MELHOR QUE A PS4? RESPOSTAS NA ANÁLISE COMPLETA

FUTURO
EPSON MOVERIO
OS ÓCULOS QUE DÃO UMA TAREIA AOS GOOGLE GLASS

PROCESSADOR
CORE I7-4790K
A INTEL VOLTA A QUEBRAR TODOS OS RECORDES DE DESEMPENHO

DE TOPO
GALAXY TAB S
O PRIMEIRO TABLET QUE "METE O IPAD NA GAVETA"

IMPRESA Publishing
5 603846 017284 00230

ROUTERS DESATUALIZADOS; MUNICÍPIOS VULNERÁVEIS

Um estudo do Politécnico de Beja apurou que as redes dos municípios podem ser bloqueadas facilmente por hackers sem experiência. Um quarto das falhas detetadas permite ataques de execução de códigos **por Hugo Séneca**

Há 308 câmaras municipais em Portugal. Há uma elevada probabilidade de todas terem antivírus e firewall – mas há também uma elevada probabilidade de todas estarem vulneráveis a um ataque de negação de serviço lançado com um simples comando junto do router, que pode ser efetuado por um único internauta, e que até nem terá de ter especiais conhecimentos sobre a matéria. Não é o único sinal alarmante: um inquérito realizado por um finalista do Mestrado de Engenharia de Segurança Informática da Politécnico de Beja apurou que 23% de todas as vulnerabilidades detetadas podem ser usadas para desviar tráfego, quebrar a autenticação ou executar o código remoto nas redes informáticas das câmaras.

Daniel Franco, o autor do estudo, ilustra o problema com um episódio sucedido no inquérito efetuado às câmaras sob anonimato: «Perguntámos aos responsáveis das câmaras se estavam atentos às atualizações dos routers e um deles respondeu-nos que "em equipa que ganha, não se mexe". A verdade é que as pessoas apenas têm cuidado com os servidores, computadores pessoais e antivírus, mas com os equipamentos ativos de rede não tomam medidas de segurança».

Hoje, o router serve de porta de acesso ao exterior para todas as organizações. Rui Miguel Silva, professor do Instituto Politécnico de Beja, recorda que o panorama tende a tornar-se mais complexo com a expansão das "redes planas", que são controladas na totalidade por um único router.

«(Ao contrário do inquérito do Politécnico de Beja), quem quiser lançar um ataque não vai fazer perguntas às vítimas. Qualquer miúdo conseguiria obter as respostas que precisa, através de ferramentas que existem na Net», acrescenta Rui Miguel Silva.

Rui Miguel Silva e Daniel Franco, nos laboratórios do Instituto Politécnico de Beja: «As câmaras têm usado equipamentos com vulnerabilidades conhecidas há anos»

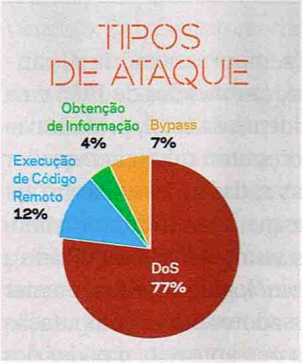
INQUÉRITO ANÓNIMO

No inquérito anónimo, as questões incidiam sobre o modelo, a marca, o sistema operativo e upgrades dos routers usados pelos municípios. Com as respostas dos serviços dos municípios, os investigadores ficaram em condições de fazer as devidas comparações com os alertas e notícias que vão saindo ao longo do tempo sobre as vulnerabilidades que afetam os diferentes modelos/sistemas operativos dos routers usados pelas câmaras. O processo não é muito diferente daquele que um hacker faz quando escolhe uma potencial vítima: há uma análise da máqui-

na usada e do sistema operativo usado, e depois segue-se a procura de vulnerabilidades conhecidas que poderão ser exploradas.

Só que no caso de Daniel Franco, este trabalho de "sapa" foi feito com propósitos académicos, recorreu a um inquérito com propósitos benéficos, e não a ferramentas de scan (Nmap é provavelmente a mais conhecida) que fazem o diagnóstico das diferentes máquinas sem que os donos os saibam. Das 308 câmaras inquiridas, apenas 89 responderam ao inquérito. Daniel Franco optou por centrar o estudo apenas nas respostas de 62 das 89 câmaras que aceitaram participar no inquérito. «Mais de 60% dos routers camarários são Cisco. E foi só por serem a maioria que optámos por nos centrar apenas nos routers desta marca. Também há vulnerabilidades nos routers de outras marcas. Todas estas marcas têm falhas muito semelhantes», descreve Daniel Franco.

Com uma amostra que corresponde a um quinto de todos os municípios do País, a Daniel Franco ficou em condições de tirar a seguinte conclusão: «As câmaras têm estado a usar equipamentos de rede que correm sistemas operativos com vulnerabilidades conhecidas há anos». A esta conclusão junta-se outra questão que não pode ser respondida por inquéritos académicos: «Este trabalho apenas permite obter informação sobre vulnerabilidades que já conhecidas e que foram reportadas».



Rui Miguel Silva acredita que o panorama não será melhor nas câmaras que não participaram no inquérito. «Poucas serão as que fazem as atualizações dos equipamentos ativos de rede. Acredito que quase todas as 308 câmaras têm falhas deste tipo». O especialista admite que, também no setor privado, as atualizações dos routers sejam igualmente descuradas.

Daniel Franco já definiu um objetivo de estudo de um futuro inquérito: «Queremos fazer o mesmo tipo de análise aos switches usados pelas câmaras. Neste caso, já poderemos analisar ataques lançados a partir do interior de uma rede, que conseguem quebrar barreiras lógicas criadas por VLAN (Virtual Local Area Network), ou que permitem o sniffing do tráfego», promete Daniel Franco.

DICAS A SEGUIR

No Politécnico de Beja é conhecido como «hackmóvel» - mas nos últimos tempos tem sido apresentado como «demonstrador de vulnerabilidades» em routers. A par do inquérito aos equipamentos de rede, os investigadores do Ubinet criaram uma solução que permite mostrar como é que as vulnerabilidades de um router podem ser exploradas. O demonstrador, que por enquanto está confinado a equipamento Cisco, pretende servir de ferramenta de análise e monitorização de casos reais. Daniel Franco apresenta várias dicas que poderão ajudar a evitar problemas: **1-** manter o equipamento com as mais recentes atualizações; **2-** desligar os serviços do router que não são necessários; **3-** fazer sempre uma cópia de segurança da última configuração da rede; **4-** análise constante dos registos de conexões que o router vai fazendo; **5-** analise padrões de tráfego em busca de comportamentos anómalos (exemplo: grande volume de dados enviados para um destino suspeito); **6-** manter as passwords devidamente cifradas e proceder substituição de passwords com regularidade.

EM NEGAÇÃO DE SERVIÇO

No inquérito lançado por Daniel Franco, as câmaras eram instadas a indicar marcas, modelos, versões de sistema operativo e atualizações. O inquérito contou com a participação de 89 câmaras - mas apenas incidiu sobre 62 que usam equipamentos da Cisco. Entre todas as câmaras há um ponto em comum: a vulnerabilidade a ataques de negação de serviço (DoS). Os DoS costumam ser lançados por várias máquinas (muitas delas infetadas) em simultâneo com o objetivo de congestionar um site ou uma rede. Ou seja, o sucesso dos ataques não está relacionado com a existência de uma vulnerabilidade. Só que nas câmaras que participaram o inquérito o cenário é diferente: trata-se de uma vulnerabilidade intrínseca ao sistema operativo do router, que permite que uma única pessoa, com um mínimo de familiaridade informática, execute um comando que bloqueia toda a rede informática. A negação de serviço totaliza 77% de todas as falhas detetadas pelos investigadores alentejanos. Os restantes 23% correspondem à soma de vulnerabilidades que permitem o desvio do tráfego, à intrusão ou à execução de códigos remotamente. «Os DoS podem bloquear uma rede inteira, mas os ataques de execução remota de códigos são mais críticos, visto que permitem alterar configurações de rede e até desviar tráfego», frisa Rui Miguel Silva. Boa parte das vulnerabilidades detetadas estará relacionada com a "idade" dos equipamentos: 48% dos routers têm mais de 4 anos. Rui Solheiro, secretário-geral da Associação Nacional de Municípios Portugueses (ANMP) lembra o esforço que tem sido feito, nos últimos anos, com o objetivo de equipar os municípios. O responsável da ANMP ressalva que não conhece o estudo do Politécnico de Beja, mas, lembra que «a confirmarem-se esses índices de vulnerabilidade» a situação torna-se «preocupante» e »deverá ser analisada pelos técnicos autárquicos», conclui o responsável da ANMP.