Análise de Certificados Digitais em Domínios Brasileiros

Matheus Aranha
Diogo Pereira
Artur Ziviani
Fábio Borges

Introdução e Motivação

Introdução

- Certificados digitais
- Algoritmos de criptografia
- Autoridades Certificadoras

Introdução

MENU G1 SEGURANÇA DIGITAL

‹ VEJA TODOS OS POSTS

Segunda-feira, 14/05/2018, às 17:33, por Altieres Rohr

Certificado digital do Banco Inter é revogado após chave vazar na web

Um certificado digital do Banco Inter, acompanhado da respectiva chave privada, foi publicado em um site na web e posteriormente revogado, segundo apuração do blog **Segurança Digital**. O banco Inter é o mesmo que está sendo investigado pelo Ministério Público do Distrito Federal após uma reportagem do site de tecnologia "TecMundo" afirmar que dados de vários correntistas da instituição foram obtidos em um possível ataque cibernético realizado por um invasor que teria tentado extorquir o banco cobrando um "resgate".

O certificado digital por si não é capaz de provar que o ataque e o vazamento de dados ocorreram, mas esse certificado é parte da tecnologia responsável por proteger a comunicação dos correntistas do banco com o site da instituição (bancointer.com.br). Mesmo que um ataque não tenha ocorrido, ou que o ninguém tenha usado a chave para atacar

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Revoked (keyCompromise)	2018-05-11 22:06:58 UTC	2018-12-09 22:32:55 UTC	2018-12-10 12:02:24 UTC
CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

SHA-256(Certificate) C69D1129E8514B18C6DF0850C2395F20B28C5E01398AB80D8170A0E302D34619

SHA-1(Certificate) A7BD677CD4637E8661B09647083CCCFFF9048E31

Certificate | ASN.1

Hide metadata

Run cablint

Run x509lint

Run zlint

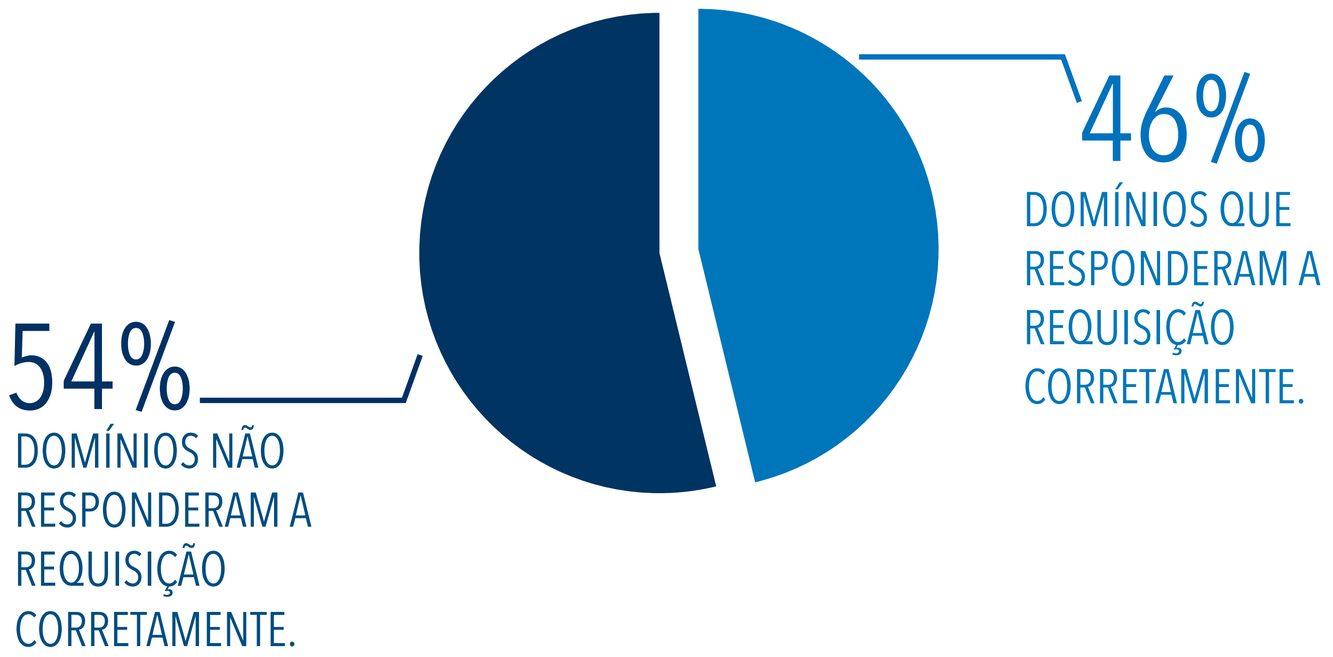
Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            93:8f:ea:34:71:ab:56:87
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 904)
            commonName               = Go Daddy Secure Certificate Authority - G2
            organizationalUnitName   = http://certs.godaddy.com/repository/
            organizationName         = GoDaddy.com, Inc.
            localityName             = Scottsdale
            stateOrProvinceName      = Arizona
            countryName              = US
        Validity
            Not Before: Aug 18 14:10:03 2017 GMT
            Not After : Aug 18 14:10:03 2019 GMT
        Subject:
            commonName               = *.bancointer.com.br
            organizationName         = BANCO INTERMEDIUM SA
            localityName             = BELO HORIZONTE
            stateOrProvinceName      = Minas Gerais
            countryName              = BR
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:8e:ac:88:55:c5:ab:45:e3:eb:43:32:6d:ab:25:
                    7a:2c:35:86:1c:57:73:47:63:5f:0a:72:8d:0f:f0:
                    bc:f6:23:65:77:50:b1:f1:71:dd:80:61:59:3f:f8:
                    b5:ed:d0:00:c1:31:fb:34:e0:b8:e8:ec:d0:13:48:
```

Metodologia

Metodologia

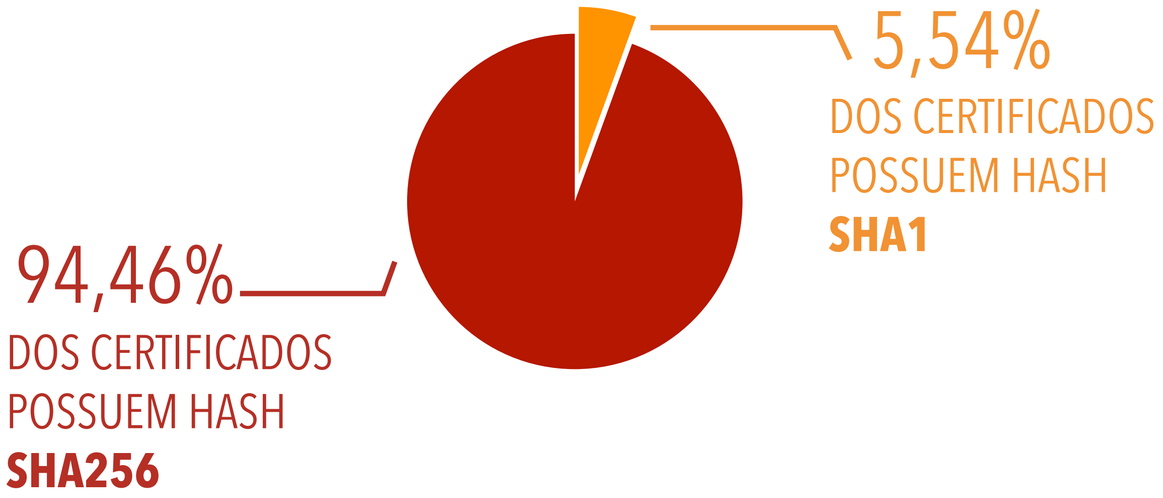
- Foram coletados certificados SSL de todos os sites com domínios de extensão *.br*
- Intervalo de tempo entre os anos de 2012 e 2013
- Totalizando 572.506 domínios



Metodologia

- No total foram calculadas aproximadamente 415 milhões de funções MDC.

- Apesar dos tamanhos de chaves inapropriados, observamos que todos os expoentes dos domínios coletados têm valores iguais a 65537.

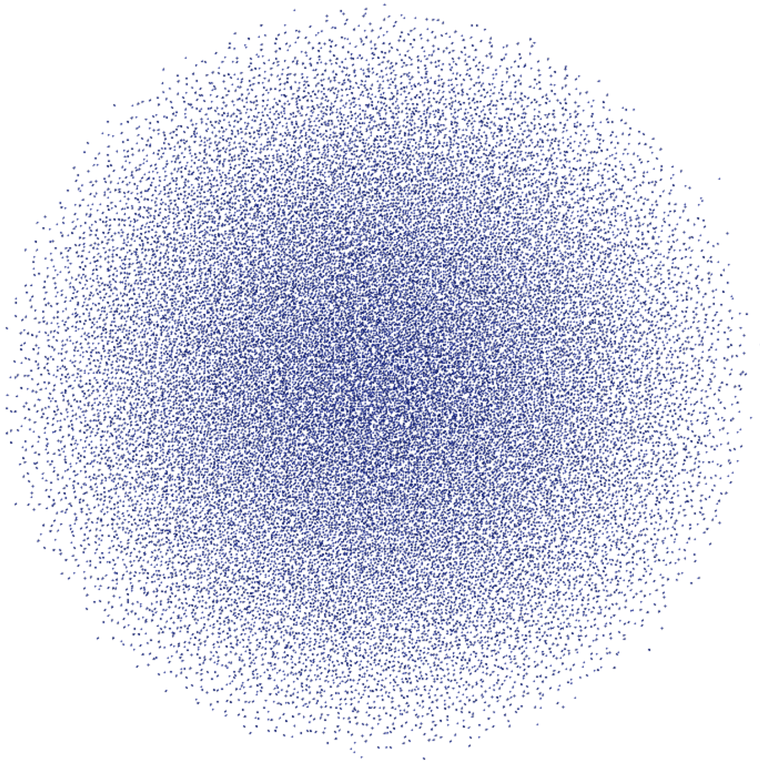


Tamanho dos módulos	Quantidade de Certificados
512 bits	101 certificados
1024 bits	4.848 certificados
1040 bits	1 certificado
2018 bits	1 certificado
2046 bits	1 certificado
2048 bits	251.080 certificados
2058 bits	1 certificado
2096 bits	1 certificado
2432 bits	1 certificado
3072 bits	14 certificados
4096 bits	8.462 certificados

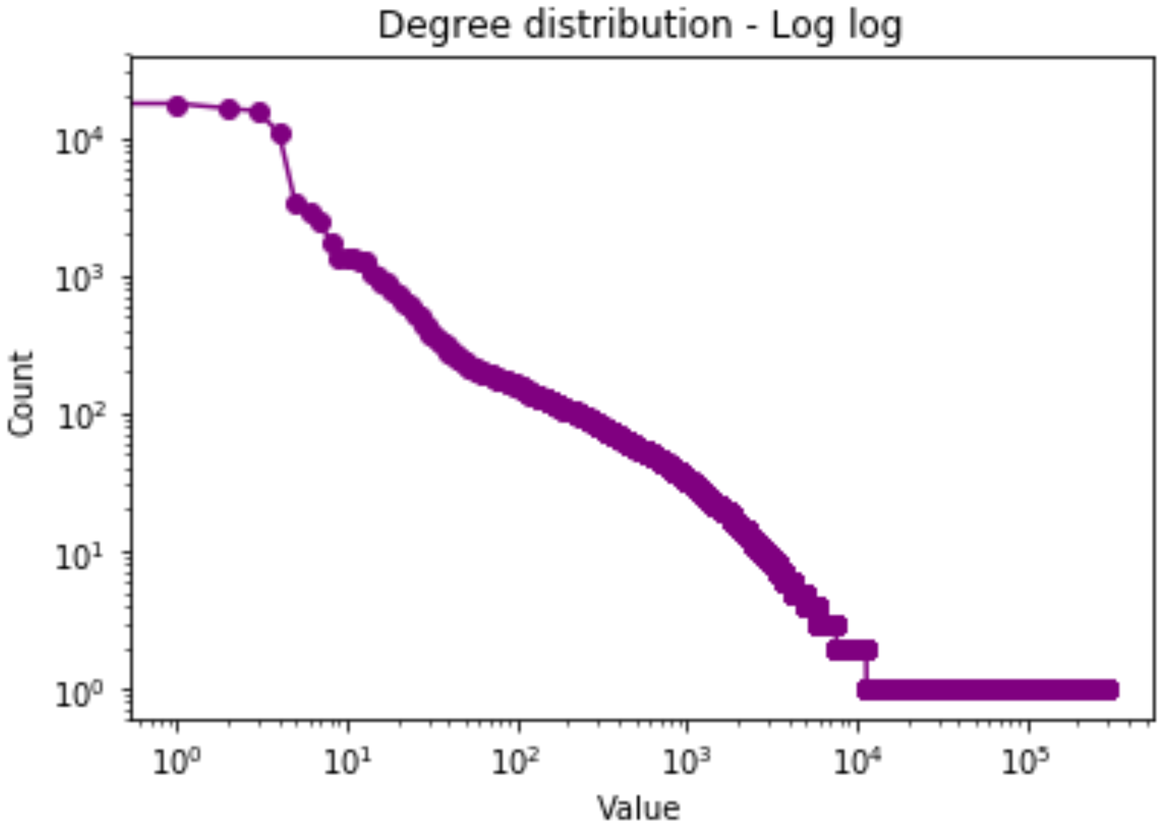
Discussões e Resultados

Primeira Representação por Grafos

- Obtivemos um grafo totalmente desconexo, ou seja, dentro do padrão já esperado.
- É possível mostrar que os algoritmos utilizados para geração de números aleatórios nos domínios brasileiros são satisfatórios.
- Os domínios brasileiros não são vulneráveis entre si para esta classe de ataque.



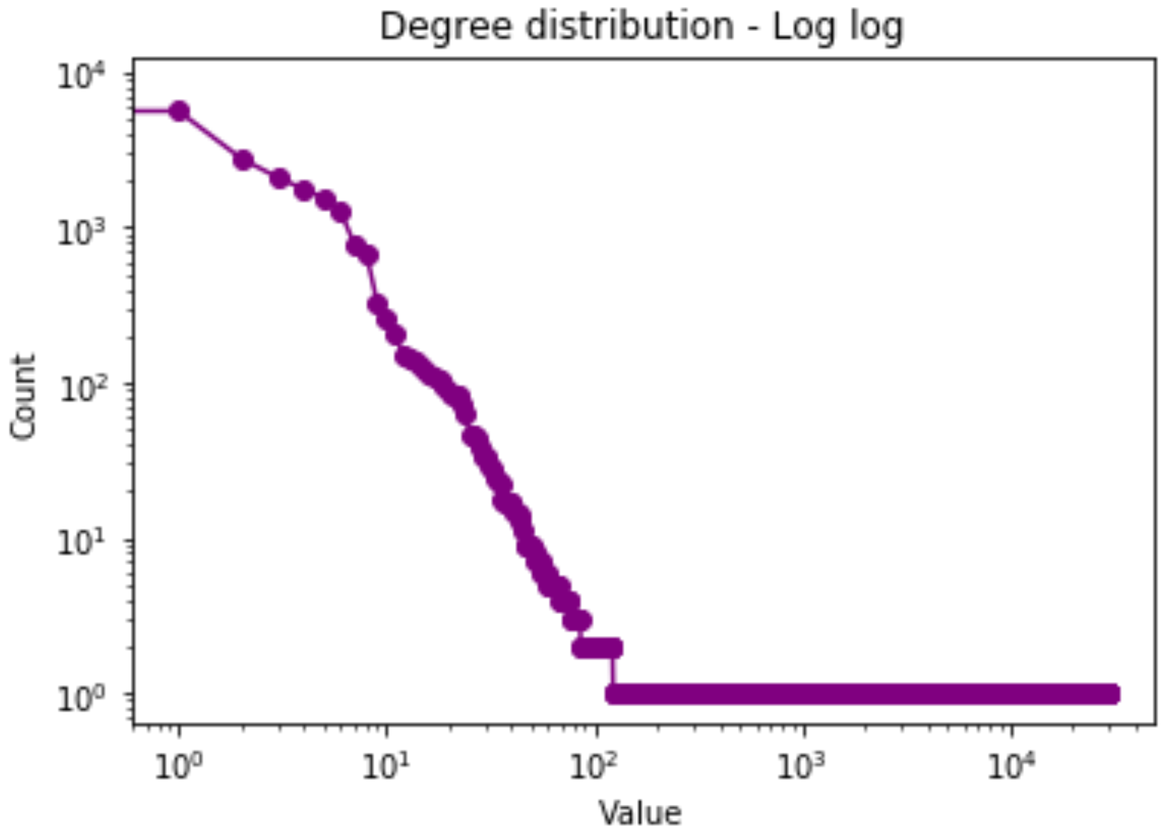
Segunda Representação pro Grafo



- Grande parte dos domínios .br (na grandeza de 10^4) compartilham o mesmo certificado SSL, consequentemente, compartilham a mesma chave privada e mesmo módulo.

- Por partilharem a mesma chave privada e módulo, se ocorrer uma falha de segurança em apenas um domínio os demais serão comprometidos.

Terceira Representação por Grafo



- A maioria dos domínios .br são certificados por grandes certificadoras de segurança ao redor do mundo, onde apenas poucas certificadoras certificam mais de 90% dos domínios.

- Caso 99% das autoridades certificadoras menos influentes atuantes nos domínios brasileiros fossem extintas, aproximadamente 90% dos domínios continuariam sendo certificados por autoridades válidas.

Conclusão

Conclusão

- Este trabalho apresenta a realização da avaliação de segurança de um requisito de segurança das chaves do RSA presentes nos certificados digitais dos domínios com extensão.br. No processo de verificação, fizemos uma análise através de Teoria dos Grafos e encontramos um resultado diferente de outros trabalhos na literatura. A diferença deve ser devida aos algoritmos de geração de números pseudoaleatórios de outros protocolos.

- Mostramos que os domínios brasileiros estão livres entre si desta classe de ataques utilizando o módulo das chaves nos certificados. Porém, é preciso realizar esta verificação em um escopo maior, pois a amostra utilizada é relativamente pequena para tirar conclusões definitivas.

Conclusão

- Mostramos que grande parte dos domínios brasileiros partilham os mesmos módulos e consequentemente os mesmos certificados, o que gera um grande problema de segurança, bastando que a chave privada de apenas um seja exposta para prejudicar os demais domínios pertencentes ao mesmo grupo.

- Por fim, mostramos a existência de uma concentração muito grande das autoridades certificadoras, sendo possível visualizar que grande parte dos domínios brasileiros são certificados por poucas autoridades. Temos que 99% das autoridades certificadoras dos certificados coletados são irrelevantes atualmente para manter os domínios brasileiros certificados.

Referencias

- Barabási, A.-L. and Pósfai, M. (2016). Network science. Cambridge University Press,Cambridge.
- Barbulescu, M., Stratulat, A., Traista-Popescu, V., and Simion, E. (2016). Rsa weak public keys available on the internet. In International Conference for Information Technology and Communications, pages 92–102. Springer.
- Boneh, D. et al. (1999). Twenty years of attacks on the rsa cryptosystem. Notices of the AMS, 46(2):203–213.
- Borges, F., Lara, P., and Portugal, R. (2017). Parallel algorithms for modular multiexponentiation. Applied Mathematics and Computation, 292:406–416.
- Braun, J. and Rynkowski, G. (2013). The potential of an individualized set of trusted cas: Defending against ca failures in the web pki. In Social Computing (SocialCom), 2013 International Conference on, pages 600–605. IEEE.
- Braun, J., Volk, F., Classen, J., Buchmann, J., and Mühlhäuser, M. (2014). Ca trust management for the web pki. Journal of Computer Security, 22(6):913–959.
- Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177):203–209.
- Lenstra, A., Hughes, J. P., Augier, M., Bos, J. W., Kleinjung, T., and Wachter, C. (2012). Ron was wrong, whit is right. Technical report, IACR.
- Martelli, A. (2017). gmpy2 library. https://github.com/aleaxit/gmpy.
- Miller, V. S. (1986). Use of elliptic curves in cryptography. In LNCS 218 on Advances in Cryptology—CRYPTO 85, pages 417–426, New York, NY, USA. Springer-Verlag New York, Inc.
- Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21(2):120–126.

Obrigado!

Perguntas?

 **github.com/mattslv/rsa-sanity-check**

 **kaggle.com/mattslv/brazil-rsa-sanity-check**