

# Massenüberwachung als Mainstream

*inkl. der Ereignisse des  
letzten Wochenendes*

Wie hat sich die Welt nach Snowden verändert?

Ben Hermann

 @benhermann

# Wer ich bin....

Dr. Ben Hermann  
Wissenschaftler an der  
Universität Paderborn

Forschung zu analytischer und  
konstruktiver Sicherheit für  
Software

Viele zu viele Filme und Bücher  
zu Spionagethemen konsumiert



 @benhermann  
[www.thewhitespace.de](http://www.thewhitespace.de)

6. Juni 2013

## US national security

Glenn Greenwald on  
security and liberty

# NSA collecting phone records of millions of Verizon customers daily

**Exclusive:** Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- [Read the Verizon court order in full here](#)
- [Obama administration justifies surveillance](#)

Glenn Greenwald

Thursday 6 June 2013 11.05 BST



**the guardian**

11. Juni 2013

A close-up video still of Edward Snowden. He is a man with short brown hair, wearing dark-rimmed glasses, a light beard, and a mustache. He is looking slightly to his left with a serious expression. The background is blurred, showing what appears to be an indoor setting.

EDWARD SNOWDEN  
NSA Whistleblower

the guardian

# Was ist da passiert?



Mit dabei sind ca. 1,7 Millionen Dateien

# Massenüberwachung

- Im letzten Vortrag: Geheimdienste und Massenüberwachung
- Heute:
  - Neue Entwicklungen und Reaktionen
  - Was die NSA mit den Angriffen des letzten Wochenendes zu tun hat.

# NSA-UA

- Erster parlamentarischer Untersuchungsausschuss des 18. Bundestags
- Eingesetzt von allen Fraktionen am 20. März 2014
- Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste aufklären
- Geladen als Zeuge seit 8. Mai 2014: Edward Snowden
- Gewährt interessante Einblicke in die Praxis des BND

# Was kam bisher heraus?

**Drei Jahre Geheimdienst-Untersuchungsausschuss: Die Aufklärung bleibt Wunschdenken, die Überwachung geht weiter**



NETZPOLITIK.ORG

- Drei Whistleblower wurden gehört
- Edward Snowden darf weiter nicht gehört werden
- “Ausspähen unter Freunden” auch beim BND absolut üblich
- Rechtsgutachten: Gesamte deutsche Auslandaufklärung rechtswidrig
- Neues BND Gesetz legalisiert und weitet aus, Budget erweitert auf 833 Mio. €

# Wen überwachen wir?

- Nachweislich hat der BND folgende Ziele aktiv abgehört:
  - Deutsche Botschaften und Diplomaten
  - Den Außenminister Frankreichs
  - Das Israelische Parlament und den Premierminister
  - USA: Außenminister Clinton und Kerry, FBI
  - so ziemlich jede europäische Regierung
  - EU Kommision, Rat und einzelne Beamte
  - UNO: IWF, WHO, UNICEF
  - Internationaler Strafgerichtshof, OPEC, OSZE
  - Rotes Kreuz, Oxfam, Welthungerhilfe
  - Diverse Banken und Ratingagenturen
  - Eurocopter, EADS, Lockheed
  - BBC, New York Times, Reuters
  - Ganz frisch: Interpol und Europol

# USA

- 29. April 2017:
  - NSA stellt angeblich anlasslose Speicherung ein
  - Künftig soll nur noch Kommunikation von oder zu einem Geheimdienstziel überwacht werden

*"NSA will no longer collect certain internet communications that merely mention a foreign intelligence target," the agency said in a statement. "Instead, NSA will limit such collection to internet communications that are sent **directly to or from a foreign target.**"*

*NSA also said it would **delete the "vast majority" of internet data** collected under the surveillance program "to further protect the privacy of **U.S. person** communications."*

# National Security Agency



```
fingerprint('demo/scenario4') =  
    fingerprint('encryption/mojahdeen2' and  
    fingerprint('browser/cellphone/iphone')
```

- \$acwitems = 'machine gun' or 'grenade' or 'AK 47'
- \$acwpositions = 'minister of defence' or 'defense minister'
- \$acwcountries = 'somalia' or 'liberia' or 'sudan'
- \$acwbrokers = 'south africa' or 'serbia' or 'bulgaria'
- \$acwports = 'rangoon' or 'albasra' or 'dar es salam'

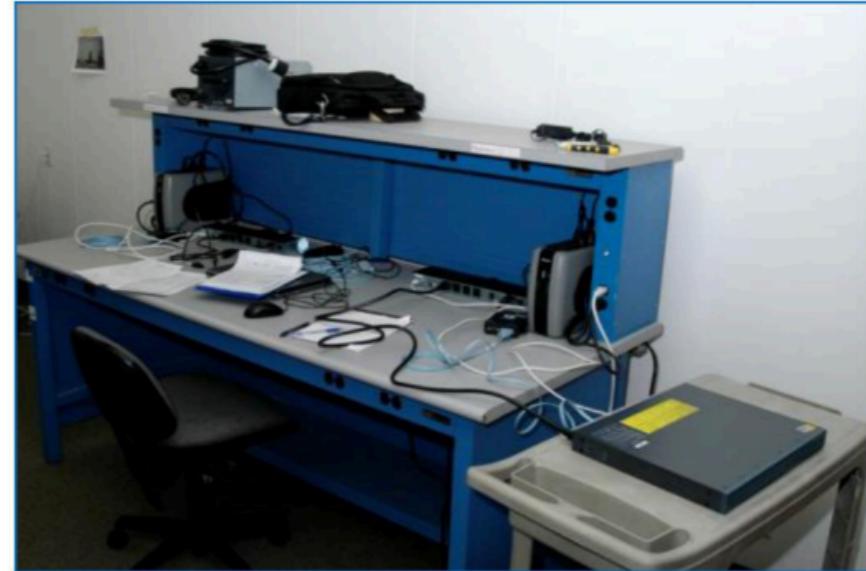
```
topic('wmd/acw/govtorgs') =  
    email_body($acwitems and $acwpositions and  
    ($acwcountries or $acwbrokers or $acwports));
```



# Tailored Access Operations



(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

# Tailored Access Operations



- Sammelt ein Arsenal an Schwachstellen in kommerzieller Software und Hardware um Zugriff auf Rechner und Netze zu erlangen
- Zielgerichtete Angriffe um Zugriff auf
  - Computer oder
  - Netzwerke zu erhalten

# Tailored Access Operations



- Wir wissen durch Snowden von dieser Abteilung
- Ziele können sein:
  - Individuelle Personen
  - Organisationen
  - Organisationen durch deren Hilfe man bessere Informationen erlangt
- Beispiele: SWIFT System, Banken

# Wie funktionieren diese Schwachstellen?

- Buffer Overflows -

```
char a[12];
unsigned int b = 8;
unsigned int c = 4;
```



# Wie funktionieren diese Schwachstellen?

- Buffer Overflows -

```
char a[12];
unsigned int b = 8;
unsigned int c = 4;
```

```
strcpy(a, "test");
```

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	00	00	00	00	00	00	00	00	00	00	00	00	08	00	04
a												b		c	

# Wie funktionieren diese Schwachstellen?

- Buffer Overflows -

```
char a[12];
unsigned int b = 8;
unsigned int c = 4;
```

```
strcpy(a, "test");
```

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
74	65	73	74	00	00	00	00	00	00	00	00	00	08	00	04
a												b	c		

# Wie funktionieren diese Schwachstellen?

- Buffer Overflows -

```
char a[12];
unsigned int b = 8;
unsigned int c = 4;
```

```
strcpy(a, "test");
```

```
strcpy(a, "muchtoo long for a");
```

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
74	65	73	74	00	00	00	00	00	00	00	00	00	08	00	04
a												b	c		

# Wie funktionieren diese Schwachstellen?

- Buffer Overflows -

```
char a[12];
unsigned int b = 8;
unsigned int c = 4;
```

```
strcpy(a, "test");
```

```
strcpy(a, "muchtoo long for a");
```

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
6D	75	63	68	74	6F	6F	6C	6F	6E	67	66	6F	72	61	04
a					b					c					

# Schwachstellen sind Waffen

- Das Wissen um eine Schwachstelle kann einen taktischen Vorteil bedeuten
- Es existiert ein Schwarzmarkt für diese Schwachstellen
- Hersteller schreiben schon Prämien für die Einsendung von Schwachstellen aus
- Führende Hersteller reagieren schon schnell, nur müssen die Nutzer diese Updates auch einspielen
- Faustregel: Altes System + Internet = Offenes System

# Waffenkontrolle?

16. August 2016

***'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?***

The New York Times

- Eine Hackergruppe namens Shadow Brokers verkündet man habe die NSA gehackt
- Nach einigen Versuchen damit Geld zu verdienen wurden die Werkzeuge im Quellcode Mitte April 2017 online gestellt
- Mit diesen Werkzeugen lassen sich Schwachstellen aktiv ausnutzen

# Warum glaubt man, dass diese Informationen echt sind?

- Die im Januar 2017 vorgestellten Details decken sich mit internen Informationen aus Snowden Dateien
- Snowden selber hat keinen Quellcode mitgenommen
- Mittlerweile steht der Programmcode zur Verfügung und es gilt als gesichert an
- Die NSA hat nicht bestätigt
- Schwachstellen für Windows und verschiedene Router-Hardware darunter

fb > show exploit	
Plugin Category: exploit	
Name	Version
Easybee	1.0.1
Easypi	3.1.0
Eclipsedwing	1.5.2
Educatedscholar	1.0.0
Emeraldthread	3.0.0
Emphasismine	3.4.0
Englishmansdentist	1.2.0
Erraticgopher	1.0.1
Eskimoroll	1.1.1
Esteemaudit	2.1.0
Eternalromance	1.4.0
Eternalsynergy	1.0.1
Ewokfrenzy	2.0.0
Explodingcan	2.0.2
Zippybeer	1.0.2

fb > show payload	
Plugin Category: payload	
Name	Version
Doublepulsar	1.3.1
Jobadd	1.1.1
Zobdoleto	1.1.1

# WannaCrypt

The screenshot shows a Windows-style dialog box with a red header bar containing the text "Ooops, your files have been encrypted!" and a language dropdown set to "English".

**What Happened to My Computer?**

Your important files are encrypted.  
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.  
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.  
You only have 3 days to submit the payment. After that the price will be doubled.  
Also, if you don't pay in 7 days, you won't be able to recover your files forever.  
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT

**Send \$300 worth of bitcoin to this address:**

115p7UMMngoj1pMvkpHjcRdfJNXj6LrLn

**Contact Us**

**Check Payment** **Decrypt**

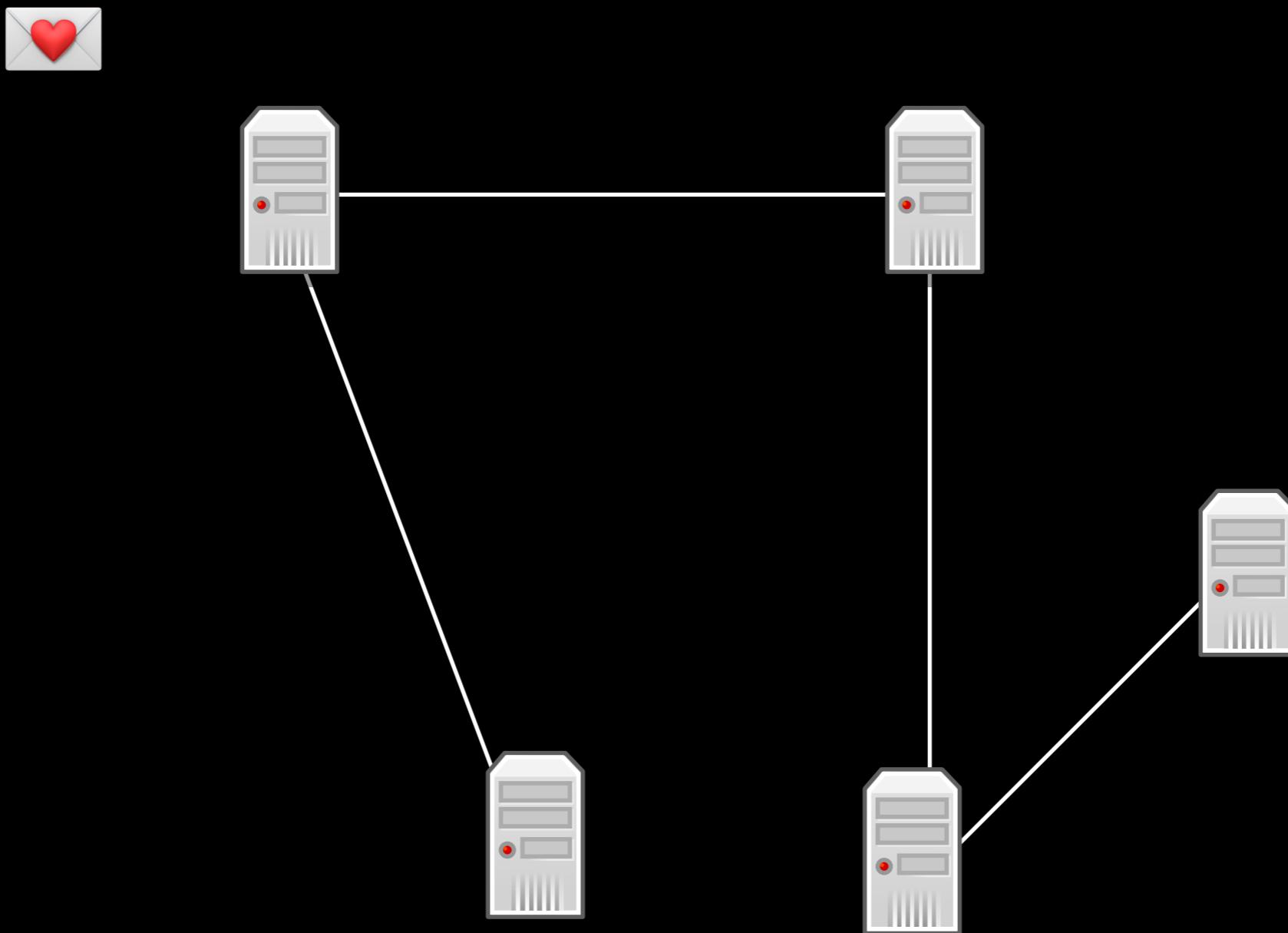
# WannaCrypt

EternalBlue

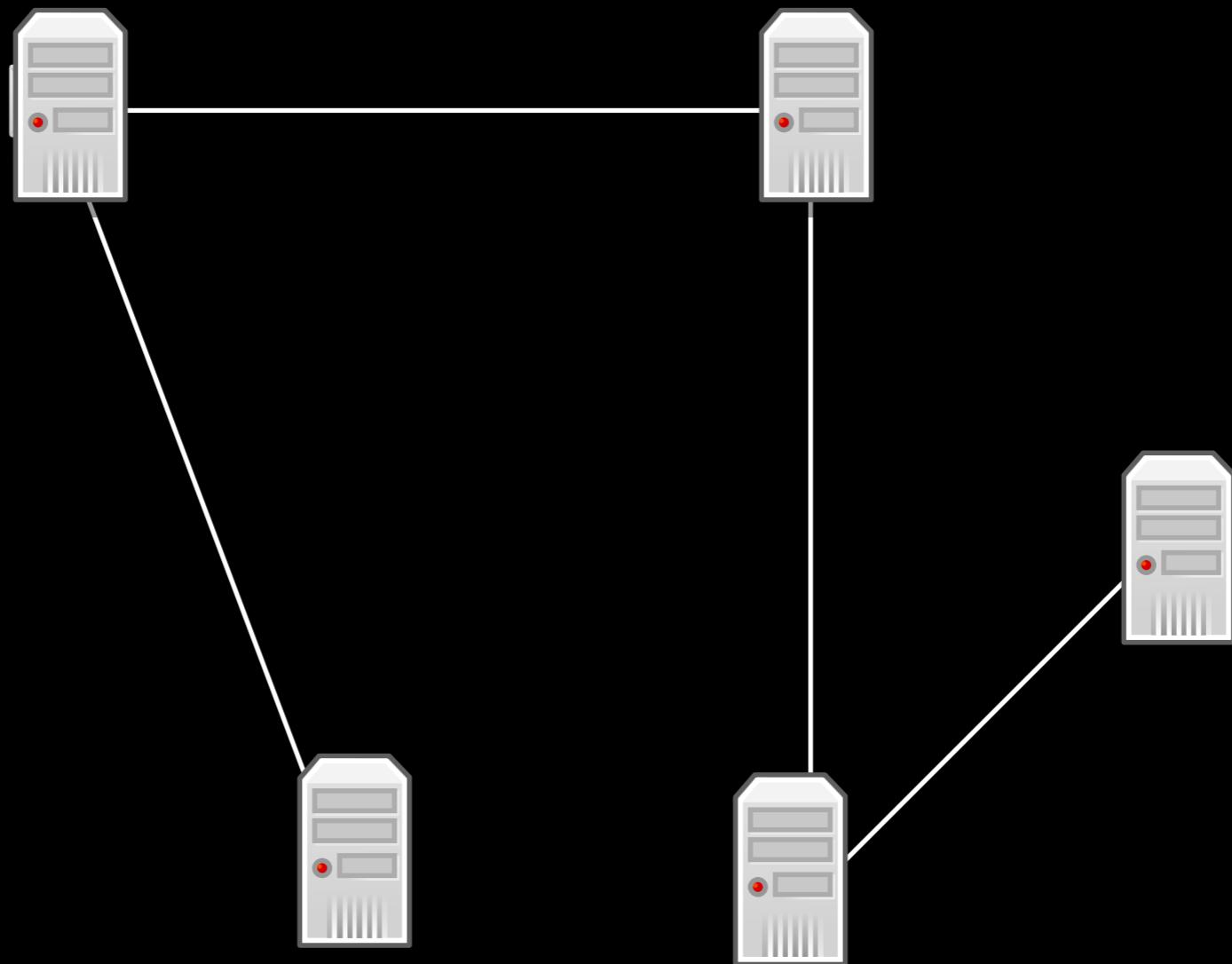
Ransomware

DoublePulsar

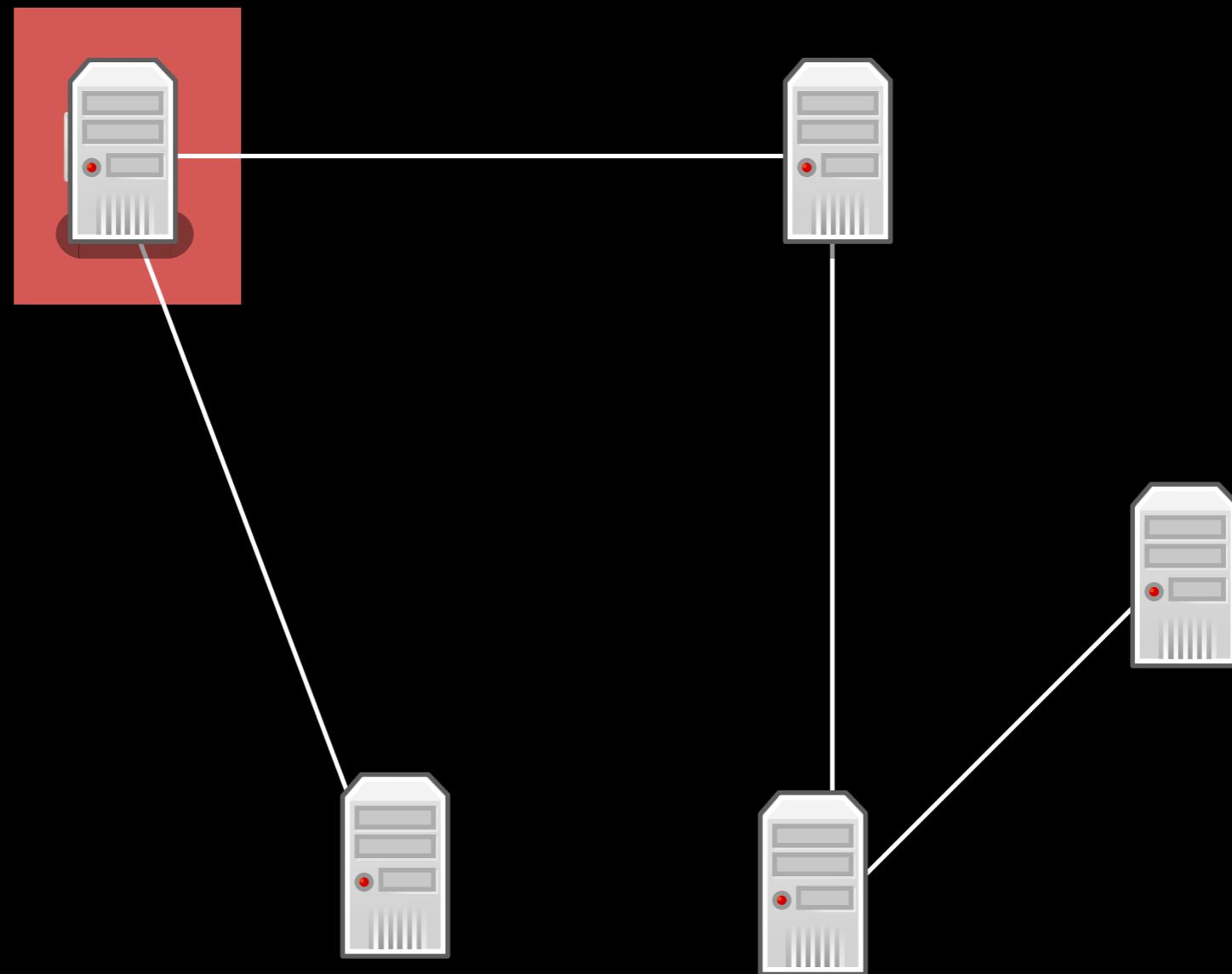
# WannaCrypt



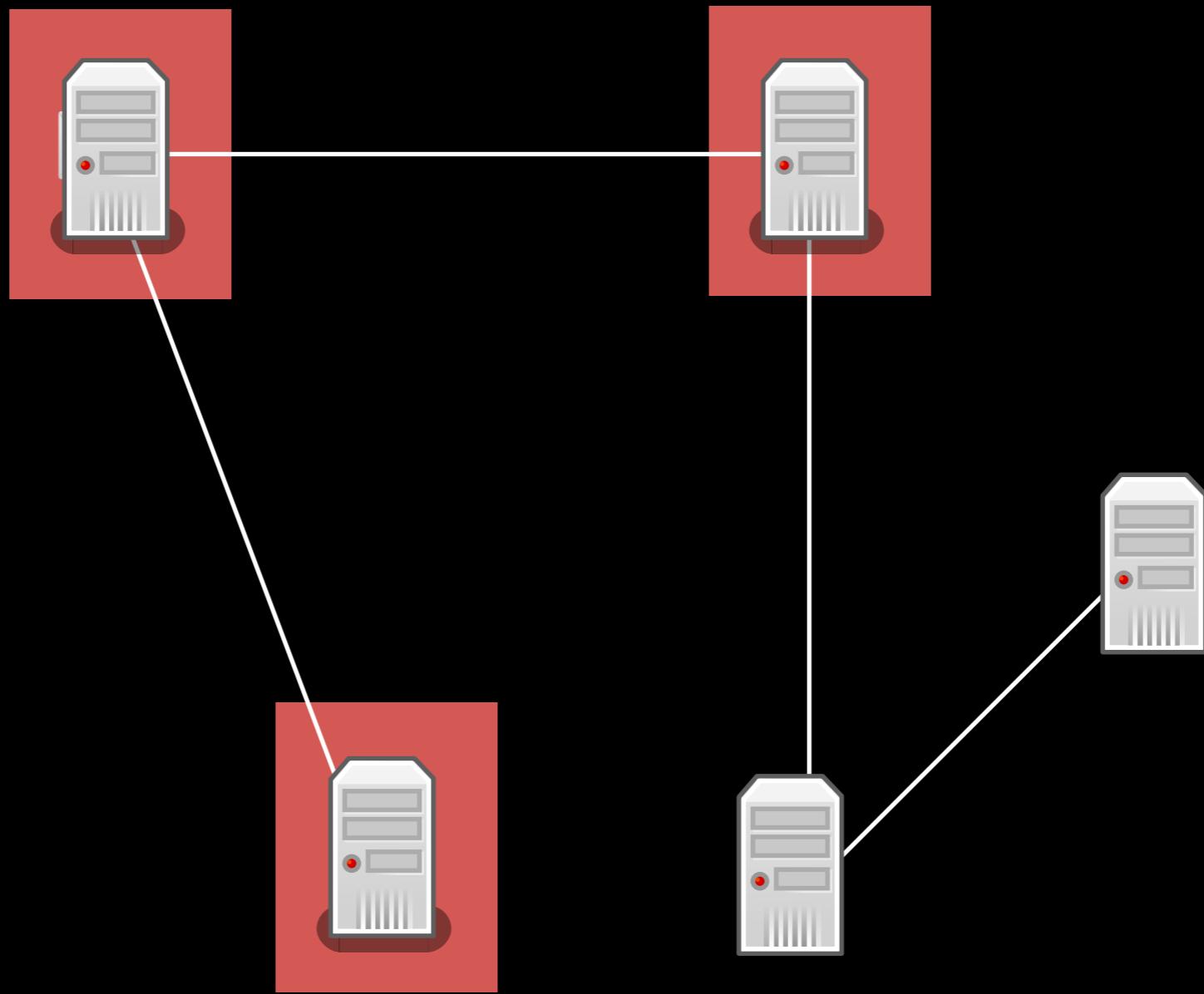
# WannaCrypt



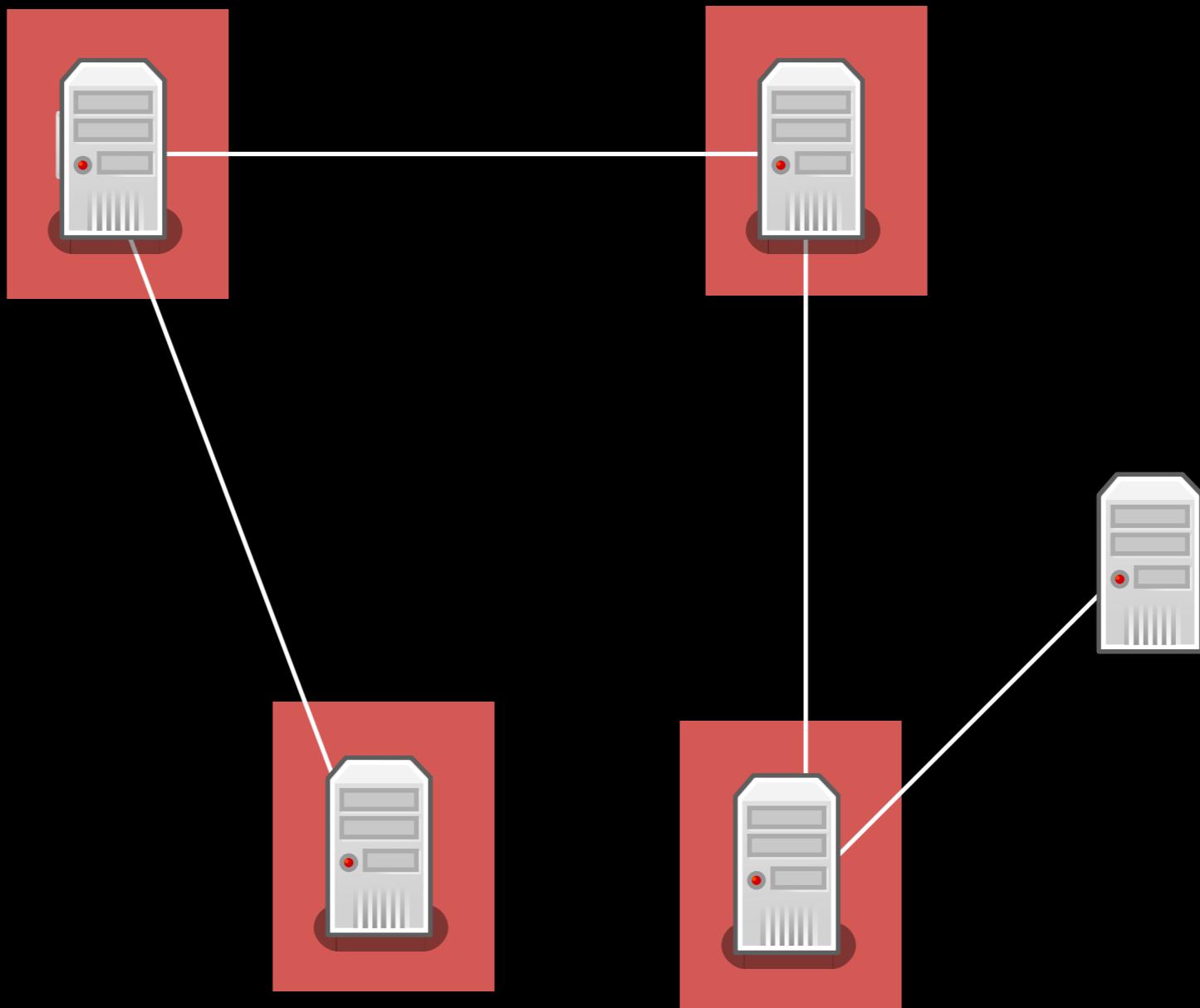
# WannaCrypt



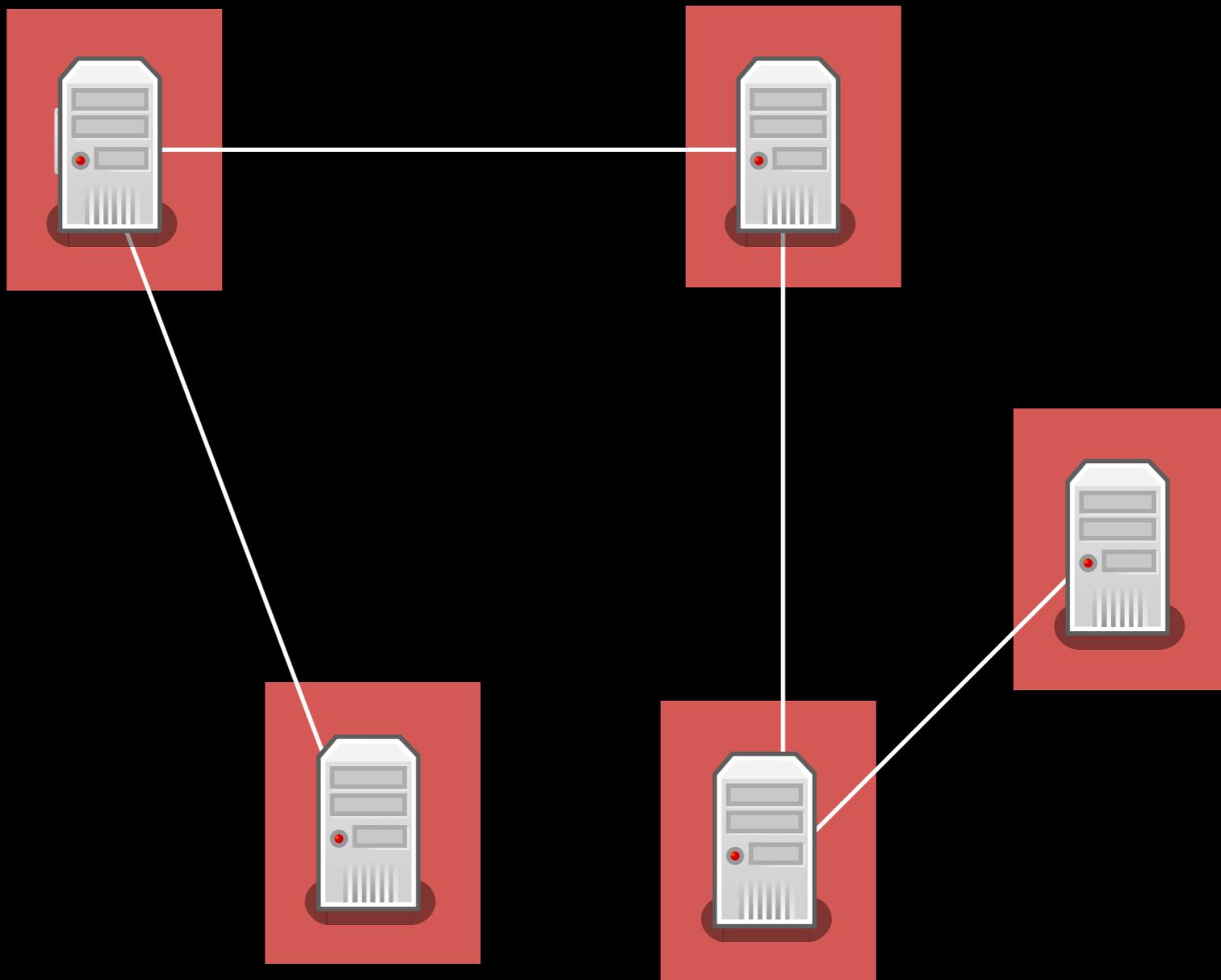
# WannaCrypt



# WannaCrypt



# WannaCrypt



# WannaCrypt



# WannaCrypt



# WannaCrypt



# WannaCrypt



# WannaCry(pt)

- Das britische Gesundheitswesen (NHS) hat 2015 aufgehört für erweiterten Windows XP Support zu zahlen, daher keine Updates
- Telefónica, Spanien (O2 in Deutschland)
- FedEx
- Russlands Innenministerium
- Nissan
- Renault
- Hitachi
- ...

# Wie hätte so etwas verhindert werden können?

- NSA veröffentlicht Schwachstellen an Hersteller
  - Direkt oder
  - Wenn solche Werkzeuge entwendet werden
- Hersteller arbeiten noch härter an ihrer IT-Sicherheit
- Forschung findet Wege solche Schwachstellen automatisch zu finden
- Nutzer aktualisieren Software

# Zusammenfassung



Was kam bisher heraus?

Drei Jahre Geheimdienst-Untersuchungsausschuss: Die Aufklärung bleibt Wunschdenken, die Überwachung geht weiter  
NETZPOLITIK.ORG

- Drei Whistleblower wurden gehört
- Edward Snowden darf weiter nicht gehört werden
- "Ausspähen unter Freunden" auch beim BND absolut üblich
- Rechtsgutachten: Gesamte deutsche Auslandaufklärung rechtswidrig
- Neues BND Gesetz legalisiert und weitert aus, Budget erweitert auf 833 Mio. €

## Waffenkontrolle?

16. August 2016  
*'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?*  
The New York Times

- Eine Hackergruppe namens Shadow Brokers verkündet man habe die NSA gehackt
- Nach einigen Versuchen damit Geld zu verdienen wurden die Werkzeuge im Quellcode Mitte April 2017 online gestellt
- Mit diesen Werkzeugen lassen sich Schwachstellen aktiv ausnutzen

A black and white satellite photograph of a large, sprawling industrial complex with numerous buildings and parking lots.

Wie funktionieren diese Schwachstellen?

- Buffer Overflows -

```
char a[12];
unsigned int b = 8;
unsigned int c = 4;

strcpy(a, "test");

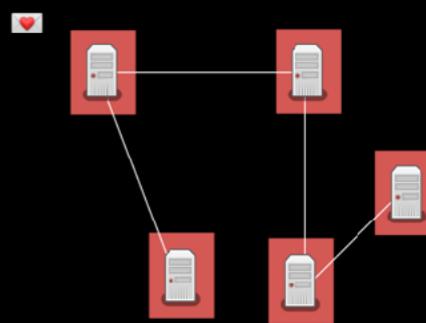
strcpy(a, "muchtoo long for a");
```

A screenshot of a debugger showing memory dump of variable 'a'. The memory dump shows the first 12 bytes of 'a' as: 00 01 02 03 04 05 06 07 08 09 0A 0B. Below it, the original code shows a buffer of length 8 being copied into 'a'. A red circle highlights the byte at index 8 of 'a', which is 0B, indicating a buffer overflow.

## WannaCrypt



## WannaCrypt



# Vielen Dank

Ben Hermann

 @benhermann

# Quellen

- <http://www.zeit.de/digital/datenschutz/2017-05/ransomware-wannacry-loesegeld-bitcoin-reaktionen>
- <https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/>
- <https://netzpolitik.org/2017/kommentar-zum-geheimdienst-untersuchungsausschuss-doch-nur-ein-ritual-das-die-illusion-einer-untersuchung-erwecken-soll/>
- <http://www.spiegel.de/politik/deutschland/bundesnachrichtendienst-ueberwachte-interpol-a-1144256.html>
- <http://www.reuters.com/article/us-usa-security-surveillance-idUSKBN17U2OF>
- <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/>
- [https://www.theregister.co.uk/2017/05/13/wannacrypt\\_ransomware\\_worm/](https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/)
- <https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/>
- [https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html?\\_r=0](https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html?_r=0)
- [https://en.wikipedia.org/wiki/The\\_Shadow\\_Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers)
- <https://theintercept.com/2015/09/17/tsa-doesnt-really-care-luggage-locks-hacked/>