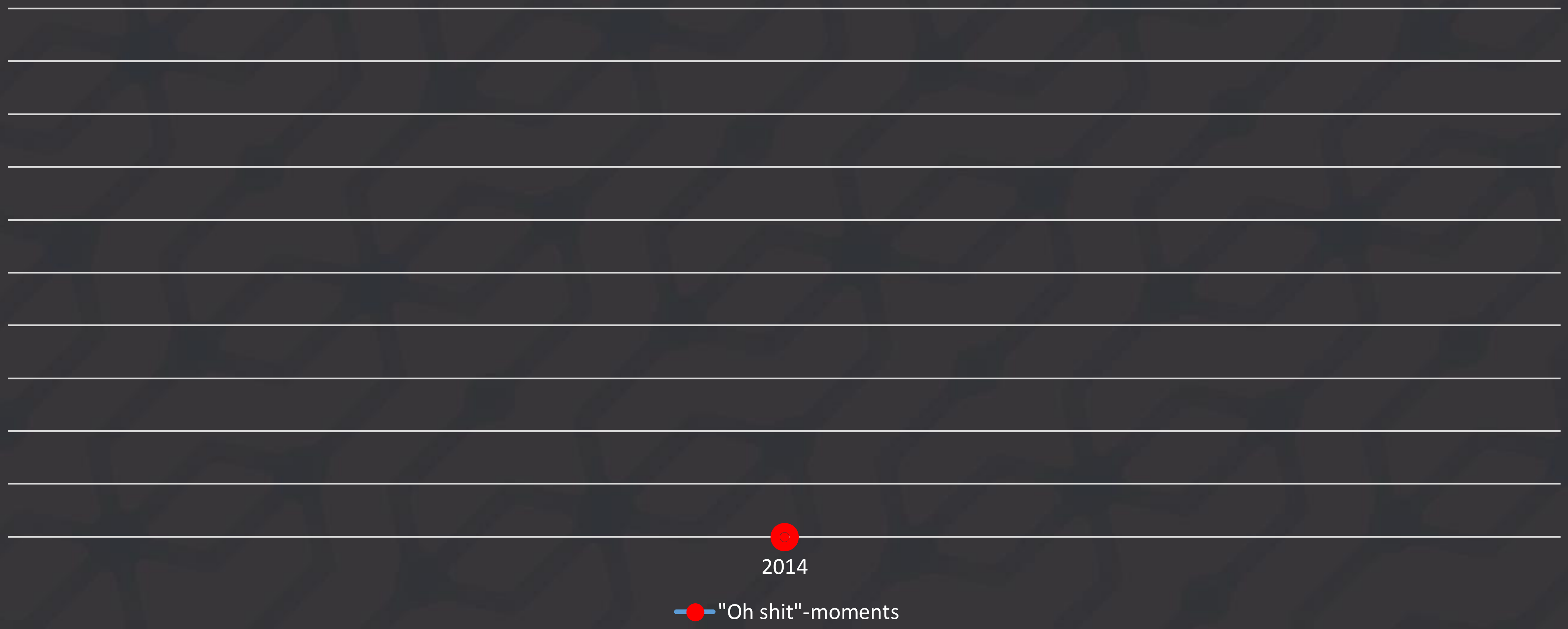
Ransomware:
What is your data worth?

Charlie Eriksen

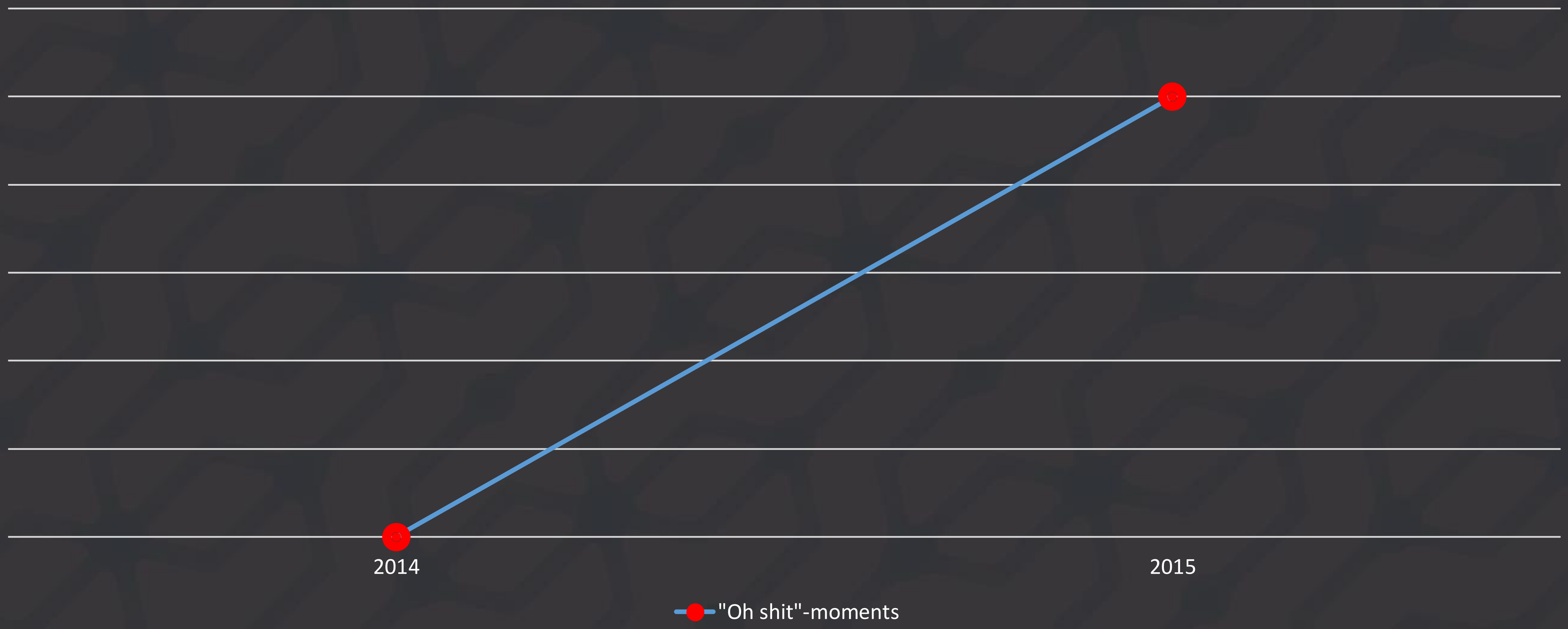
ský
Skýrslutæknifélag Íslands

SYNDIS
Creative in Security

A trend?

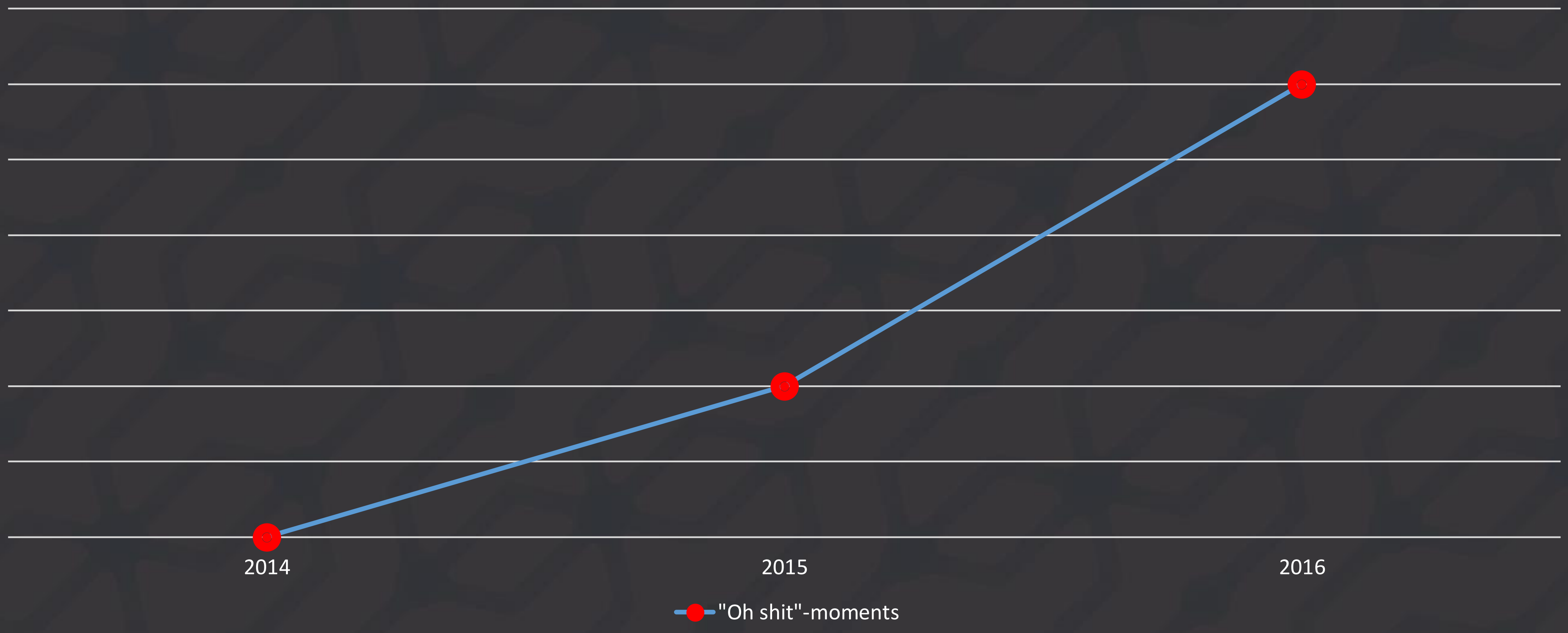


A trend?



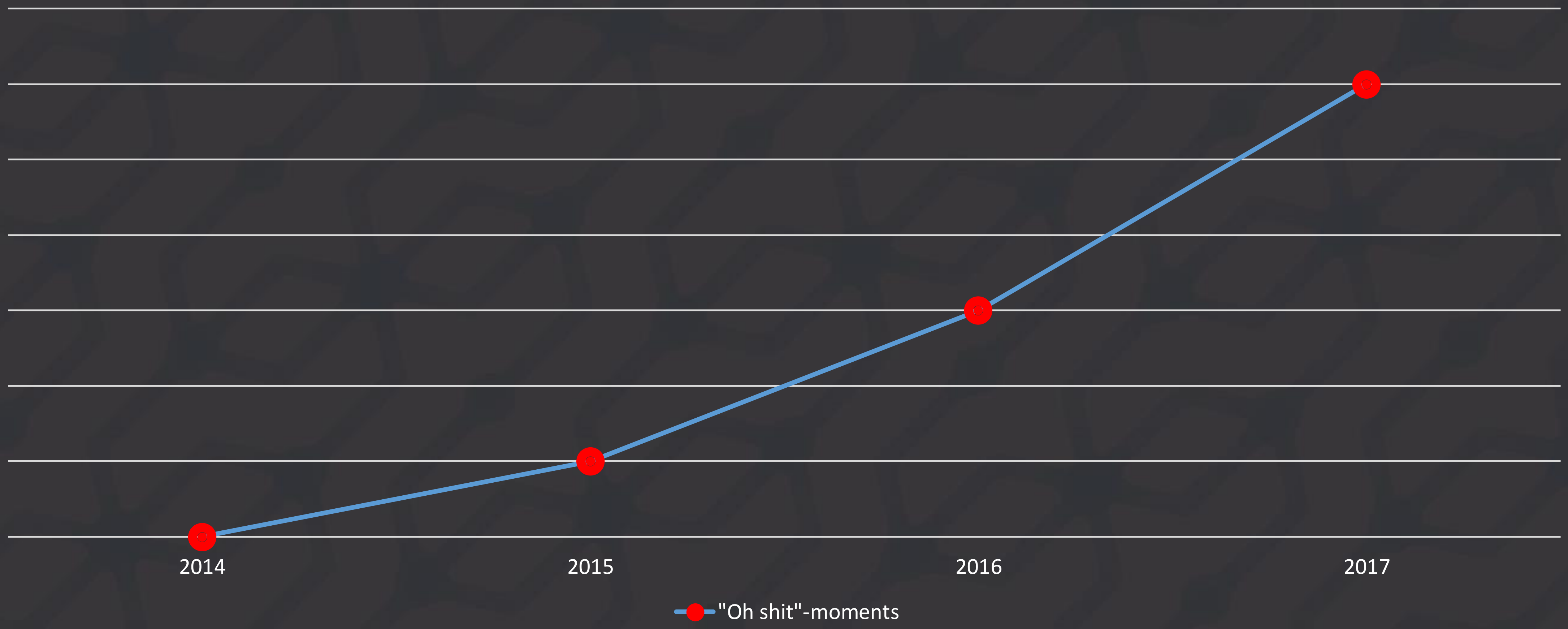
SYNDIS
Creative in Security

A trend?

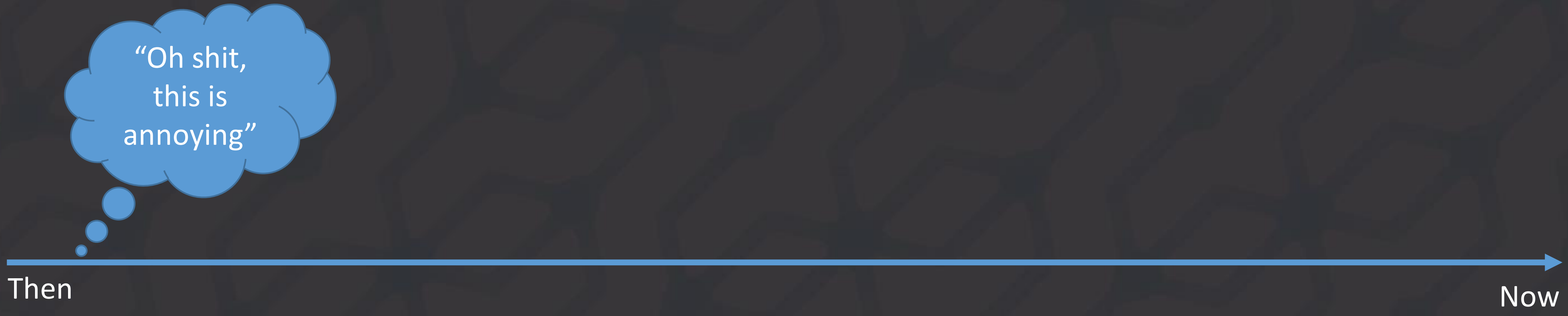


SYNDIS
Creative in Security

A trend?



Thoughts

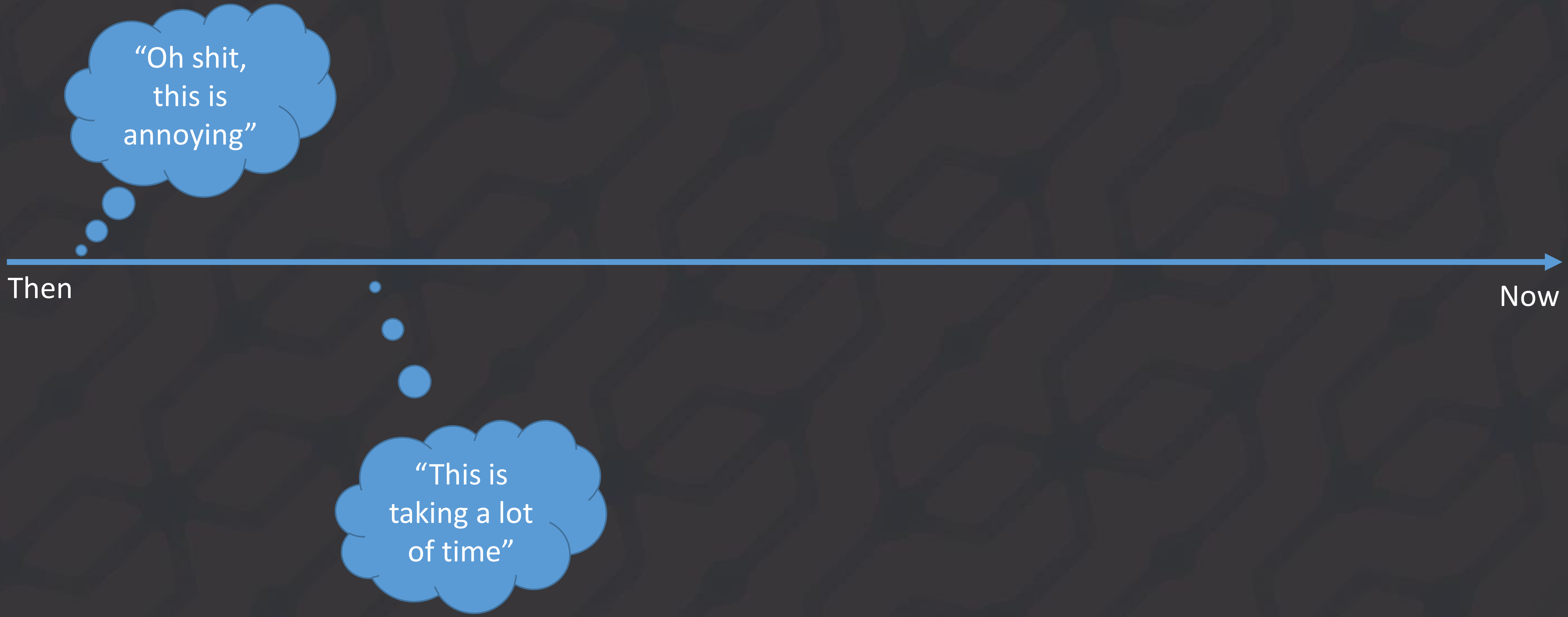


“Oh shit, this is annoying”

Then

Now

Thoughts



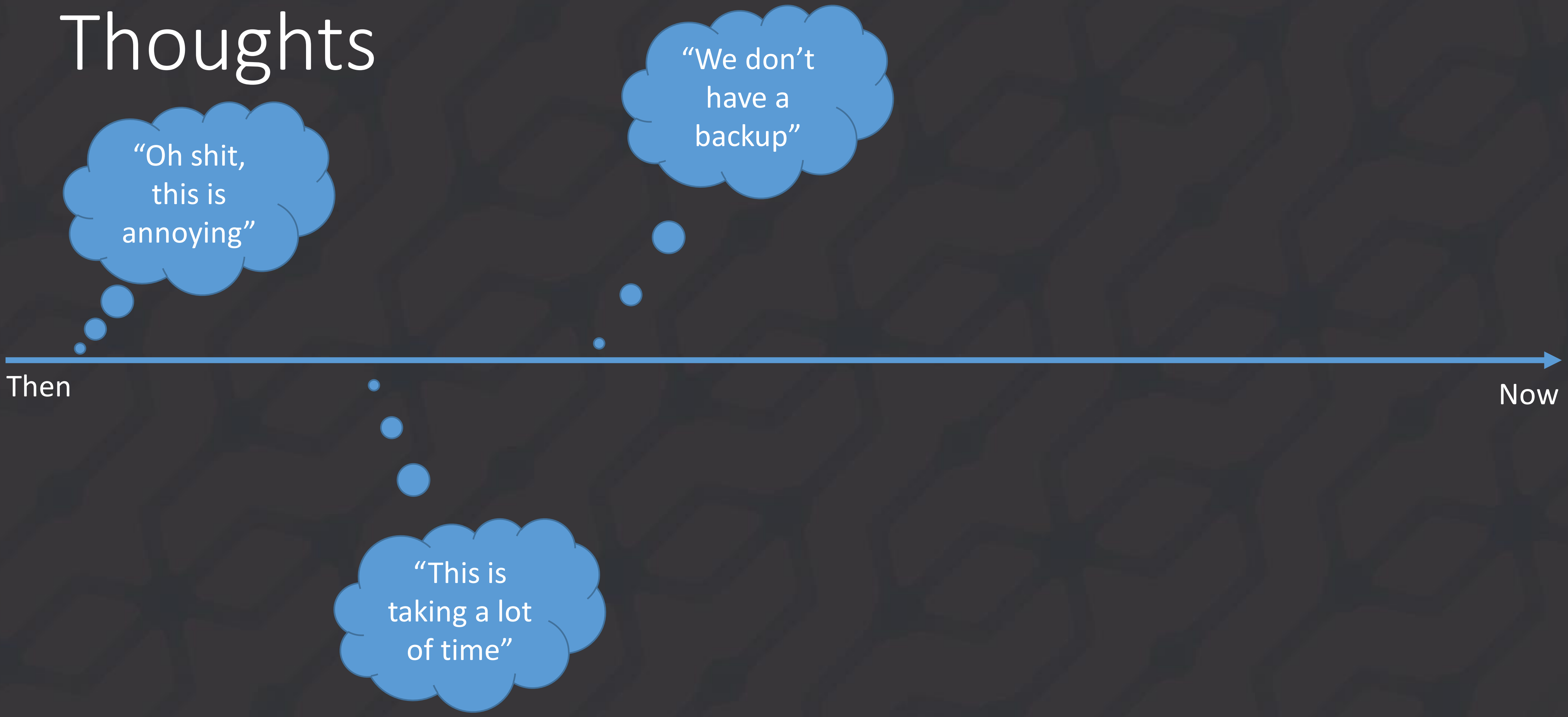
“Oh shit, this is annoying”

Then

Now

“This is taking a lot of time”

Thoughts

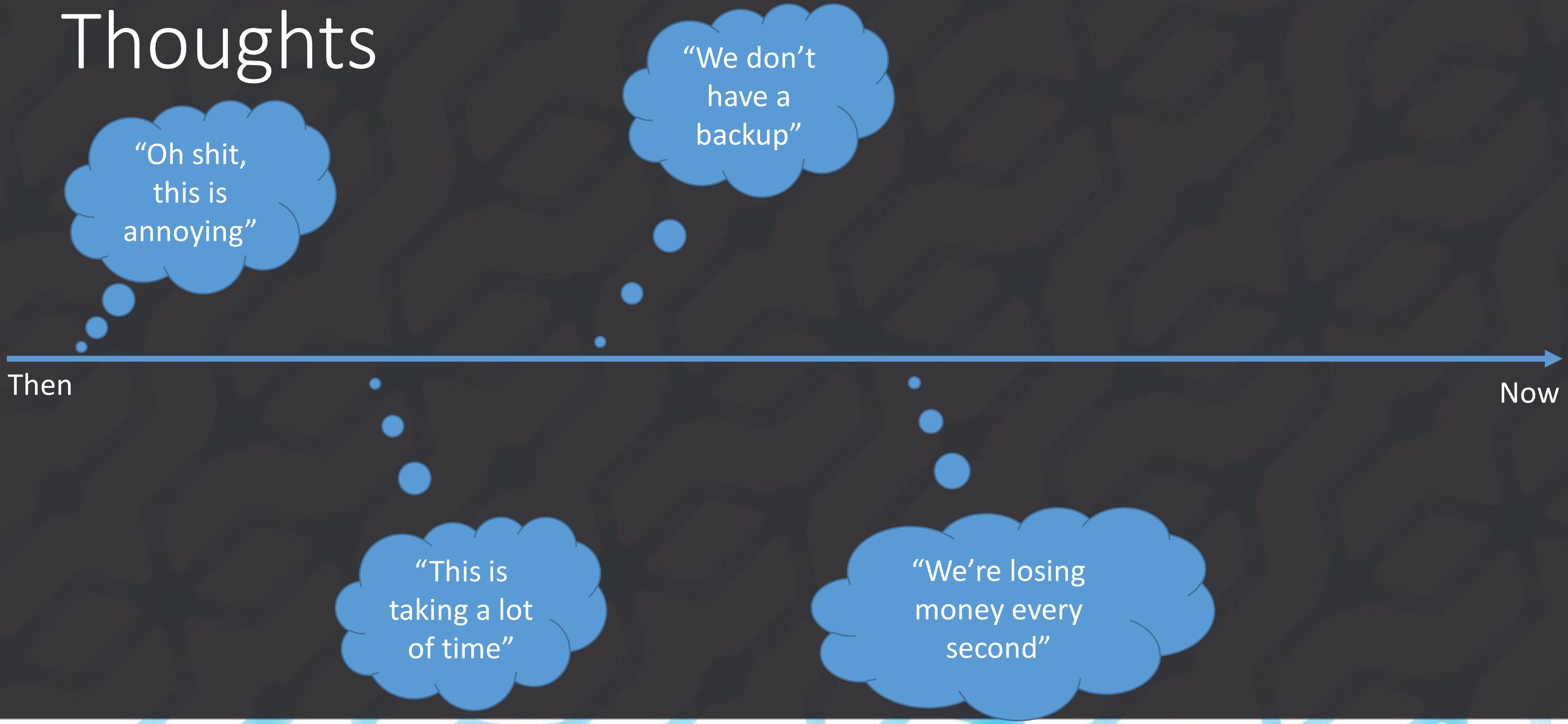


“Oh shit, this is annoying”

“This is taking a lot of time”

“We don’t have a backup”

Thoughts



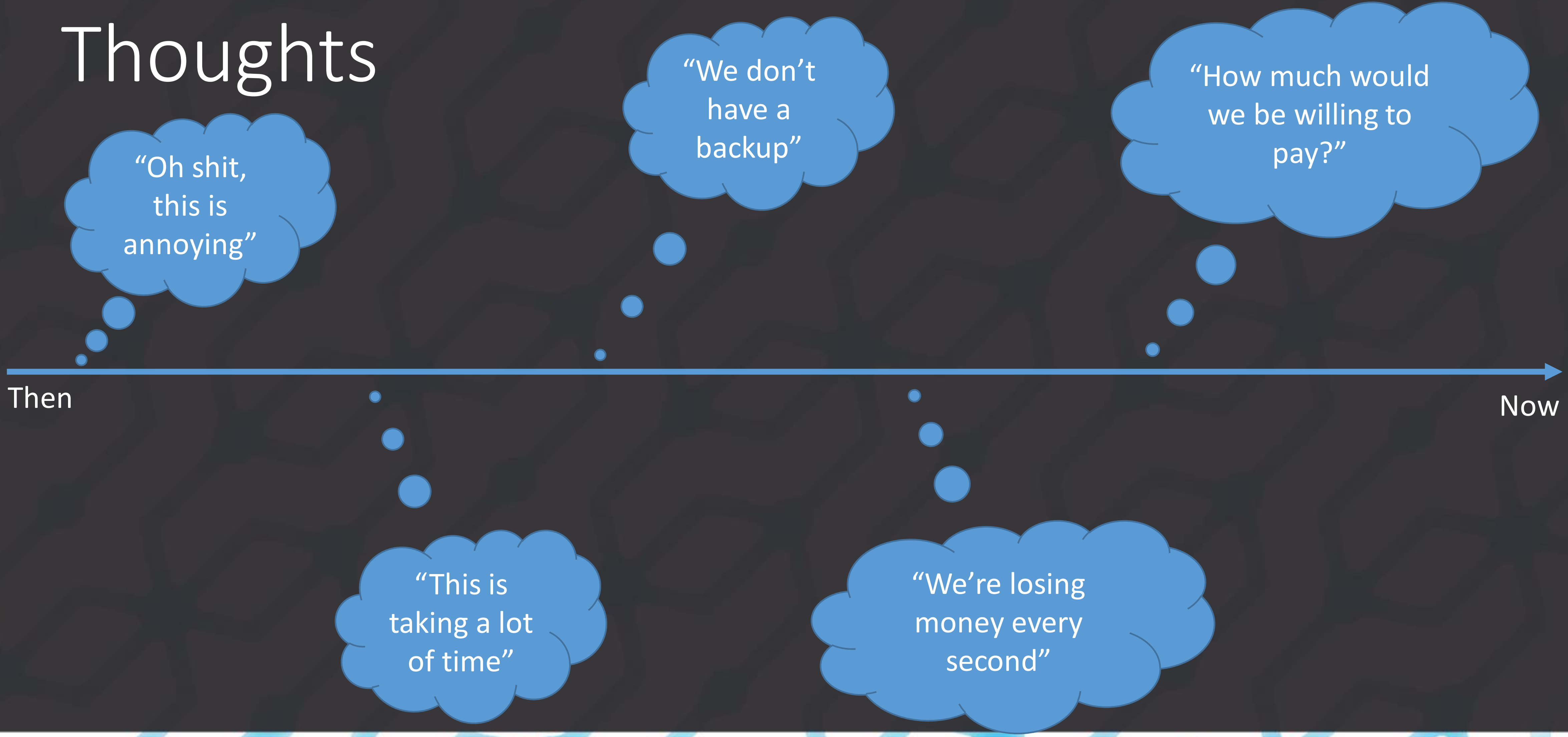
“Oh shit, this is annoying”

“This is taking a lot of time”

“We don’t have a backup”

“We’re losing money every second”

Thoughts



Then

“Oh shit, this is annoying”

“This is taking a lot of time”

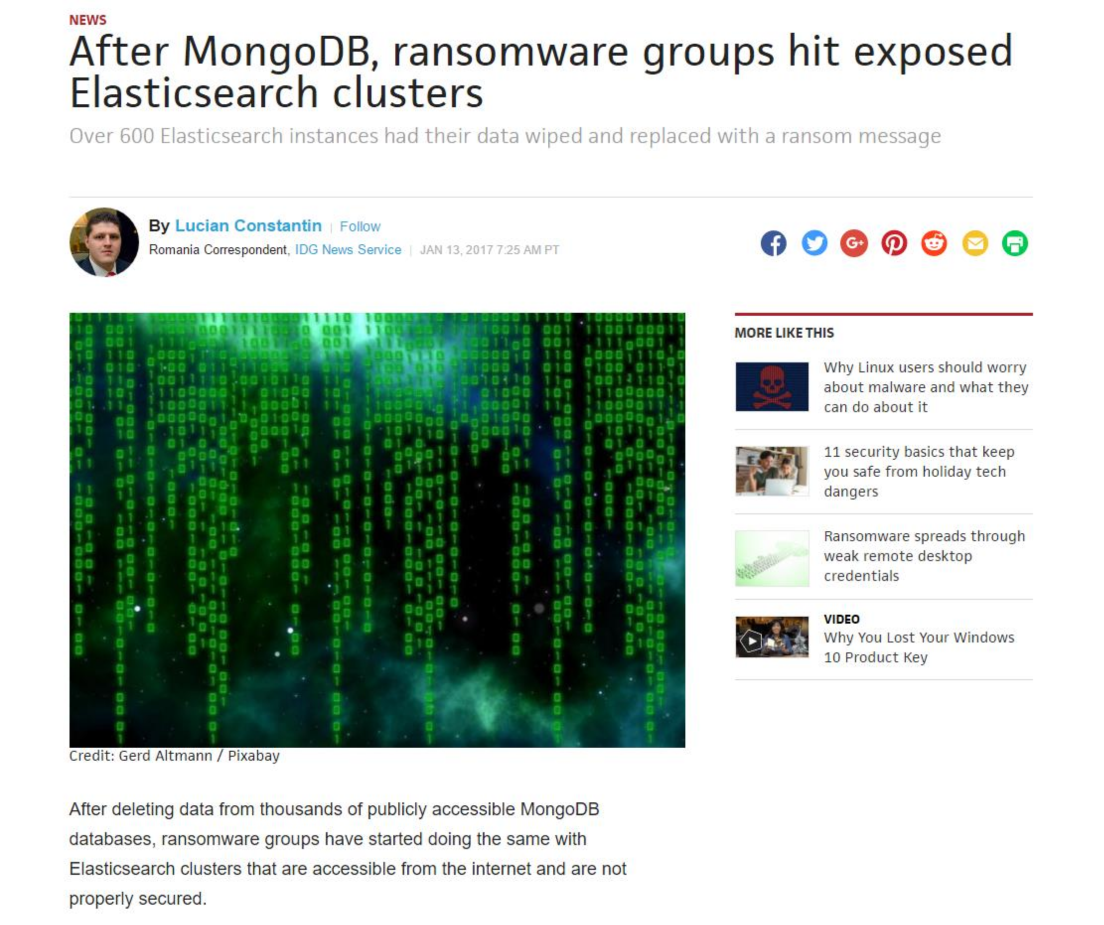
“We don’t have a backup”

“We’re losing money every second”

“How much would we be willing to pay?”

Now

Ransomware



NEWS

After MongoDB, ransomware groups hit exposed Elasticsearch clusters

Over 600 Elasticsearch instances had their data wiped and replaced with a ransom message

By Lucian Constantin | Follow
Romania Correspondent, IDG News Service | JAN 13, 2017 7:25 AM PT

Credit: Gerd Altmann / Pixabay

After deleting data from thousands of publicly accessible MongoDB databases, ransomware groups have started doing the same with Elasticsearch clusters that are accessible from the internet and are not properly secured.

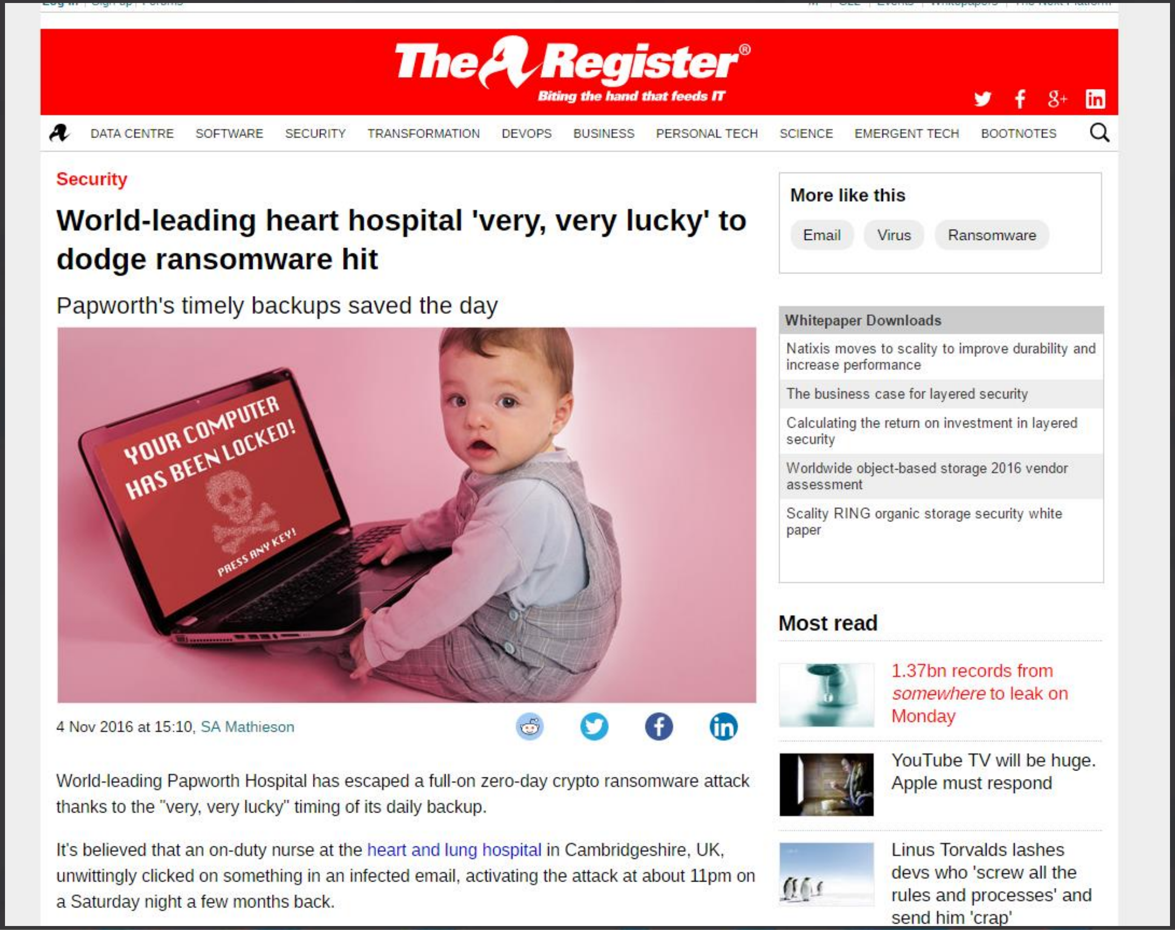
MORE LIKE THIS

- Why Linux users should worry about malware and what they can do about it
- 11 security basics that keep you safe from holiday tech dangers
- Ransomware spreads through weak remote desktop credentials
- VIDEO Why You Lost Your Windows 10 Product Key

Source: http://www.pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html

SYNDIS Creative in Security

Ransomware



The Register®
Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | TRANSFORMATION | DEVOPS | BUSINESS | PERSONAL TECH | SCIENCE | EMERGENT TECH | BOOTNOTES

Security

World-leading heart hospital 'very, very lucky' to dodge ransomware hit

Papworth's timely backups saved the day

4 Nov 2016 at 15:10, SA Mathieson

World-leading Papworth Hospital has escaped a full-on zero-day crypto ransomware attack thanks to the "very, very lucky" timing of its daily backup.

It's believed that an on-duty nurse at the heart and lung hospital in Cambridgeshire, UK, unwittingly clicked on something in an infected email, activating the attack at about 11pm on a Saturday night a few months back.

More like this

Email | Virus | Ransomware

Whitepaper Downloads

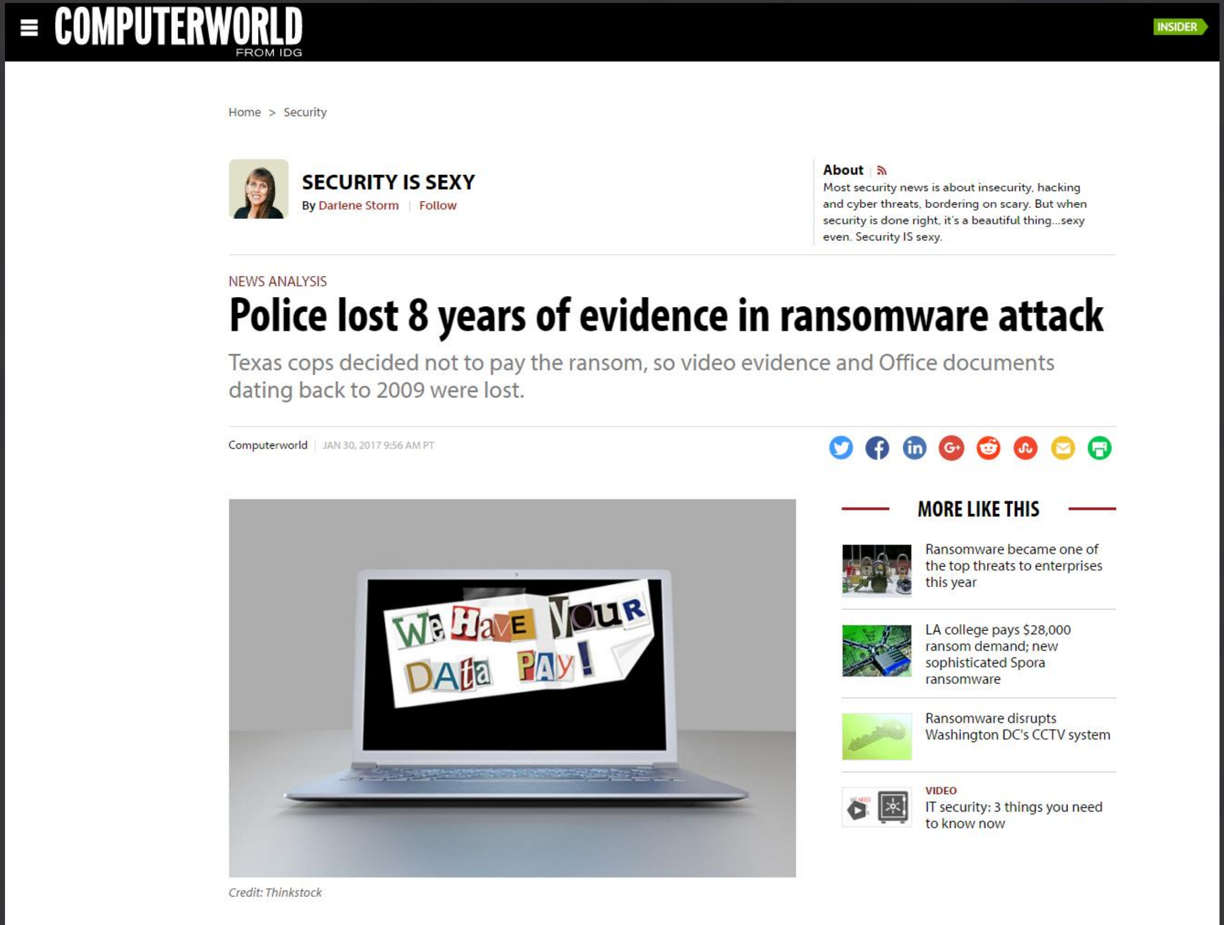
- Natixis moves to scality to improve durability and increase performance
- The business case for layered security
- Calculating the return on investment in layered security
- Worldwide object-based storage 2016 vendor assessment
- Scality RING organic storage security white paper

Most read

- 1.37bn records from *somewhere* to leak on Monday
- YouTube TV will be huge. Apple must respond
- Linus Torvalds lashes devs who 'screw all the rules and processes' and send him 'crap'

Source: https://www.theregister.co.uk/2016/11/04/papworth_ransomware_dodge/

Ransomware



COMPUTERWORLD FROM IDG

INSIDER

Home > Security

SECURITY IS SEXY

By Darlene Storm | Follow

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Police lost 8 years of evidence in ransomware attack

Texas cops decided not to pay the ransom, so video evidence and Office documents dating back to 2009 were lost.

Computerworld | JAN 30, 2017 9:56 AM PT

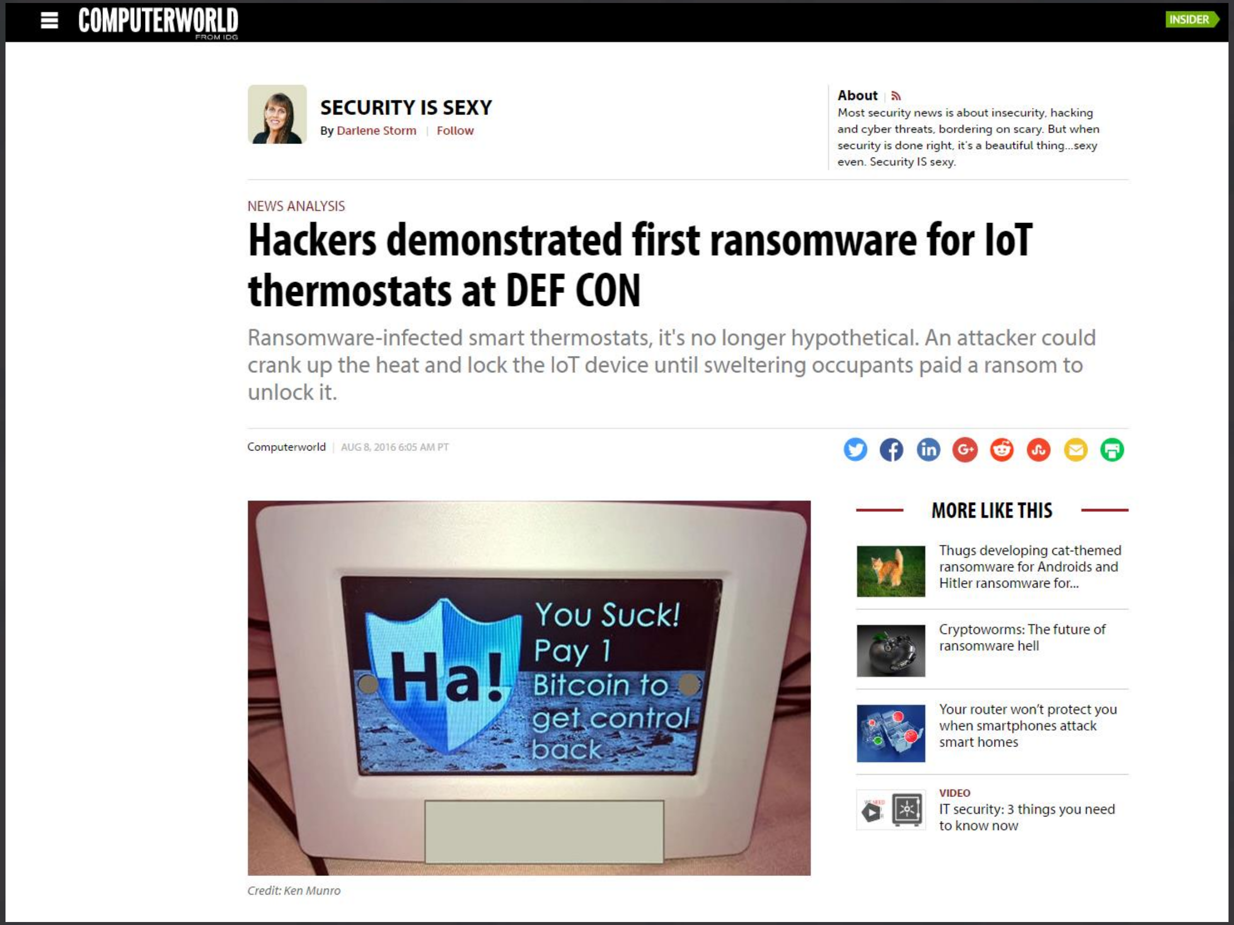
Credit: Thinkstock

MORE LIKE THIS

- Ransomware became one of the top threats to enterprises this year
- LA college pays $28,000 ransom demand; new sophisticated Spora ransomware
- Ransomware disrupts Washington DC's CCTV system
- VIDEO IT security: 3 things you need to know now

Source: http://www.computerworld.com/article/3163046/security/police-lost-8-years-of-evidence-in-ransomware-attack.html

Ransomware



COMPUTERWORLD FROM IDG

INSIDER

SECURITY IS SEXY

By Darlene Storm | Follow

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Hackers demonstrated first ransomware for IoT thermostats at DEF CON

Ransomware-infected smart thermostats, it's no longer hypothetical. An attacker could crank up the heat and lock the IoT device until sweltering occupants paid a ransom to unlock it.

Computerworld | AUG 8, 2016 6:05 AM PT

Credit: Ken Munro

MORE LIKE THIS

Thugs developing cat-themed ransomware for Androids and Hitler ransomware for...

Cryptoworms: The future of ransomware hell

Your router won't protect you when smartphones attack smart homes

VIDEO

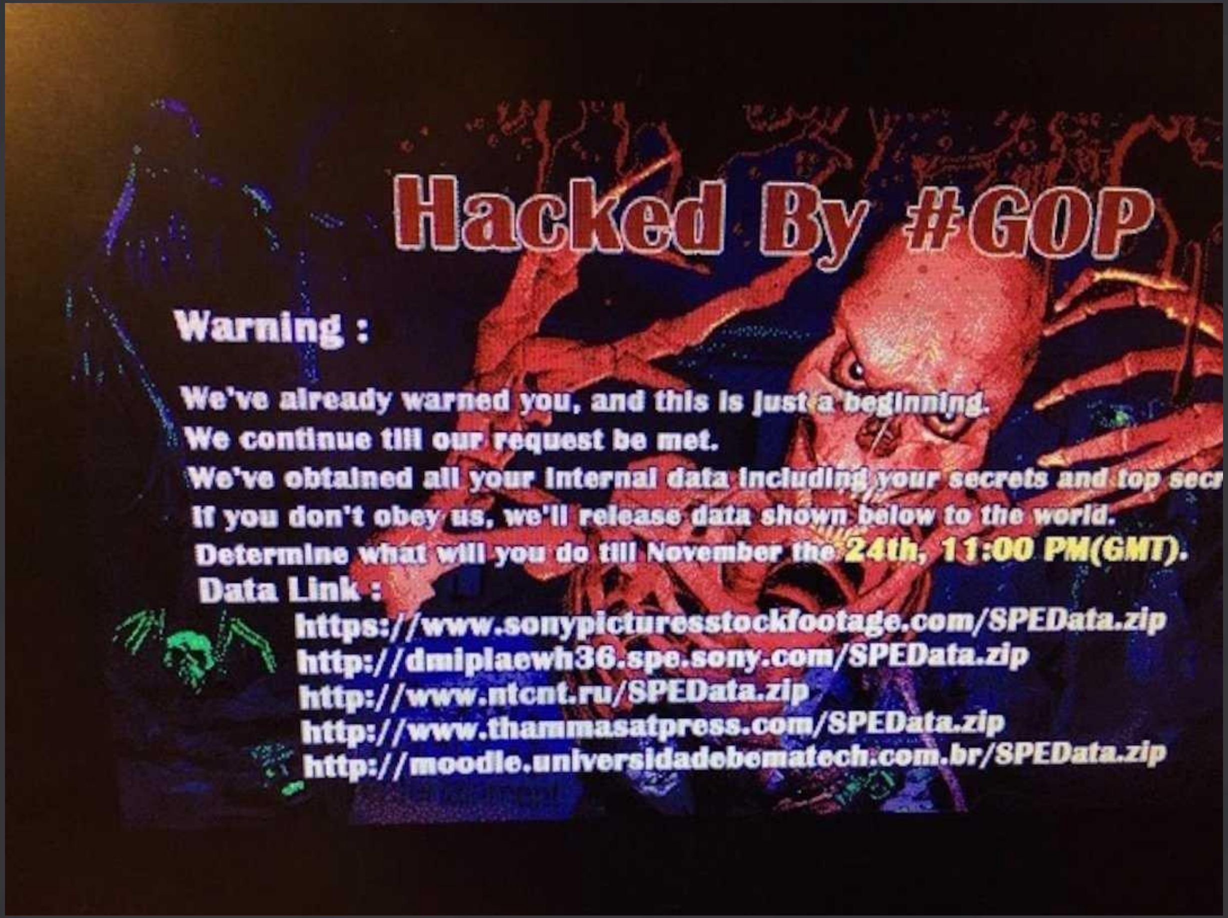
IT security: 3 things you need to know now

Source: http://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html

SYNDIS

Creative in Security

Worst case



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secr
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).

Data Link :

https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

Source: https://cdn2.vox-cdn.com/uploads/chorus_asset/file/2547914/sony-pictures-hack-6.0.jpg

What is your data worth?

What is your data worth?

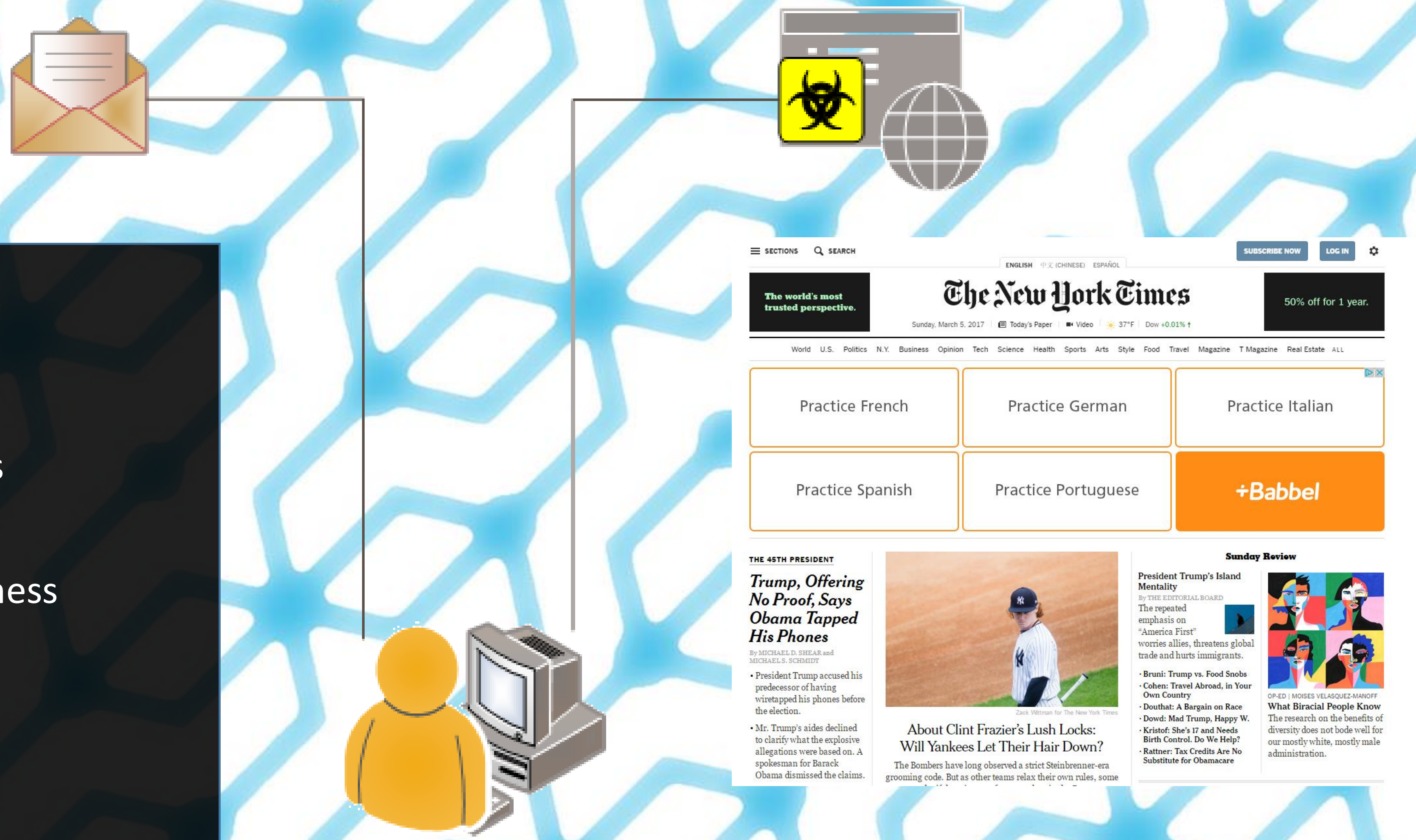
Answers to come!

How does it happen?

Source: http://i.imgur.com/YUwqfUb.gif

Infection methods

- ⚠ Out of date software
- ⚠ Unsafe browsing habits
- ⚠ Lack of security awareness



≡ SECTIONS 🔍 SEARCH SUBSCRIBE NOW LOG IN ⚙

ENGLISH 中文 (CHINESE) ESPAÑOL

The world's most trusted perspective.

The New York Times

50% off for 1 year.

Sunday, March 5, 2017 | Today's Paper | Video | 37°F | Dow +0.01% ↑

World U.S. Politics N.Y. Business Opinion Tech Science Health Sports Arts Style Food Travel Magazine T Magazine Real Estate ALL

Practice French | Practice German | Practice Italian

Practice Spanish | Practice Portuguese | +Babbel

THE 45TH PRESIDENT

Trump, Offering No Proof, Says Obama Tapped His Phones

By MICHAEL D. SHEAR and MICHAEL S. SCHMIDT

- President Trump accused his predecessor of having wiretapped his phones before the election.
- Mr. Trump's aides declined to clarify what the explosive allegations were based on. A spokesman for Barack Obama dismissed the claims.

Zack Wittman for The New York Times

About Clint Frazier's Lush Locks: Will Yankees Let Their Hair Down?

The Bombers have long observed a strict Steinbrenner-era grooming code. But as other teams relax their own rules, some

Sunday Review

President Trump's Island Mentality

By THE EDITORIAL BOARD

The repeated emphasis on "America First" worries allies, threatens global trade and hurts immigrants.

- Bruni: Trump vs. Food Snobs
- Cohen: Travel Abroad, in Your Own Country
- Douthat: A Bargain on Race
- Dowd: Mad Trump, Happy W.
- Kristof: She's 17 and Needs Birth Control. Do We Help?
- Rattner: Tax Credits Are No Substitute for Obamacare

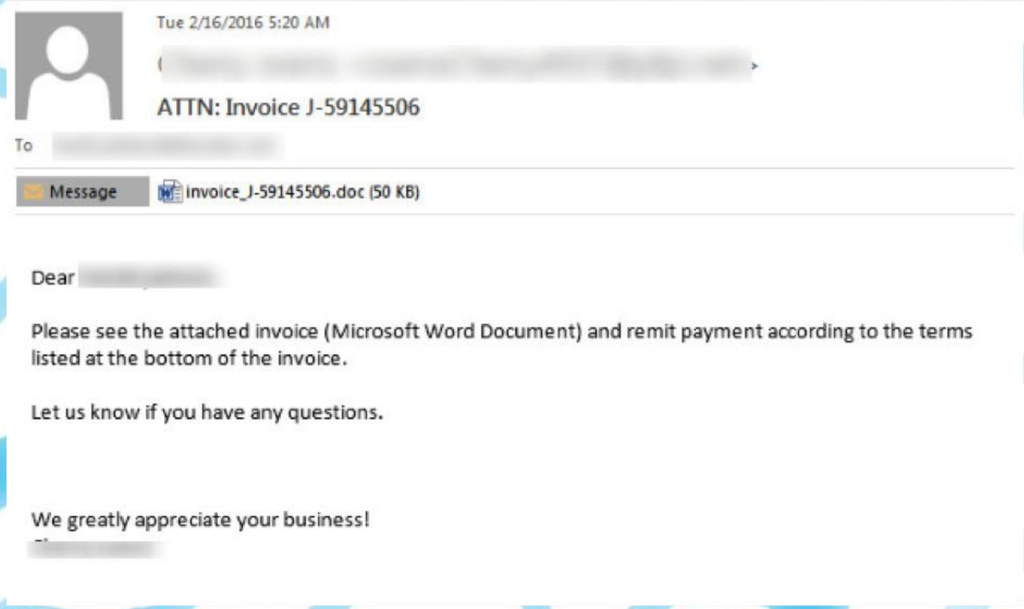
OP-ED | MOISES VELASQUEZ-MANOFF

What Biracial People Know

The research on the benefits of diversity does not bode well for our mostly white, mostly male administration.

Infection methods

- △ User running malicious executable/open malicious file
- △ Spam filter not effective
- △ Antivirus not effective
- △ Out of date software
- △ Lack of security awareness



Tue 2/16/2016 5:20 AM

[redacted]

ATTN: Invoice J-59145506

To [redacted]

Message | invoice_J-59145506.doc (50 KB)

Dear [redacted]

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!

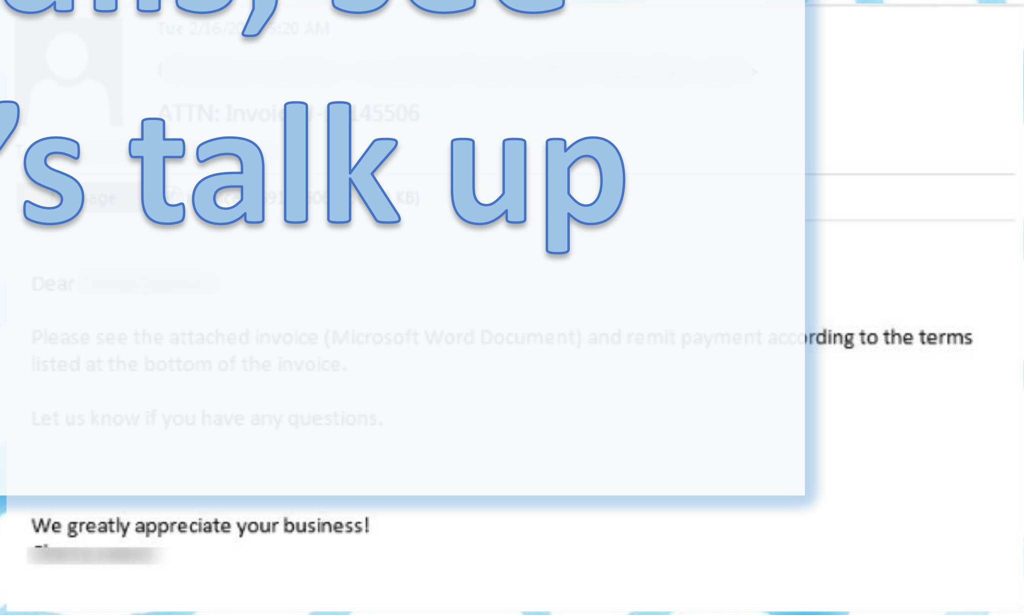
[redacted]

Source: http://www.secpod.com/blog/defeat-cryptolocker-ransomware-make-sure-your-data-is-not-taken-hostage/

Infection methods

For more details, see Kristjan Valur's talk up next

- User running malicious executable/…
- Spam filter not effective
- Antivirus not effective
- Out of date software
- Lack of security awareness



Tue 2/16/20… 5:20 AM

ATTN: Invoice … 45506

Message … Invoice … KB)

Dear [redacted]

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

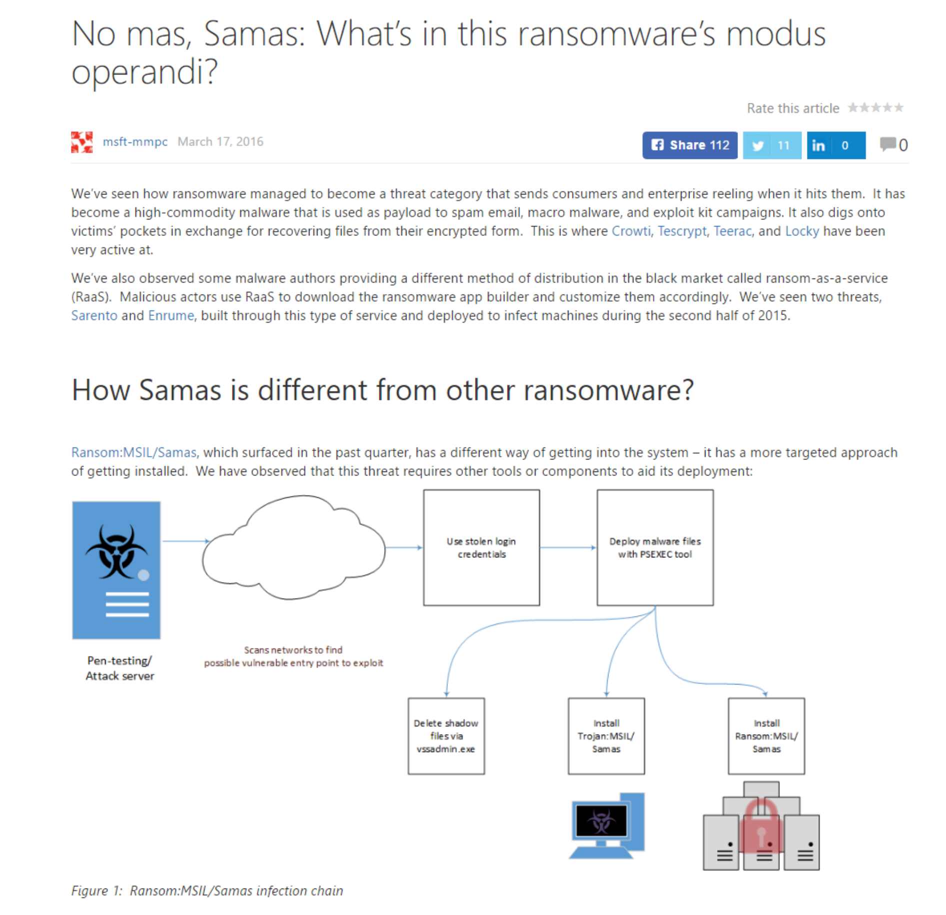
Let us know if you have any questions.

We greatly appreciate your business!

[redacted]

Source: http://www.secpod.com/blog/defeat-cryptolocker-ransomware-make-sure-your-data-is-not-taken-hostage/

Infection methods



No mas, Samas: What's in this ransomware's modus operandi?

Rate this article ★★★★★

msft-mmpc March 17, 2016

We've seen how ransomware managed to become a threat category that sends consumers and enterprise reeling when it hits them. It has become a high-commodity malware that is used as payload to spam email, macro malware, and exploit kit campaigns. It also digs onto victims' pockets in exchange for recovering files from their encrypted form. This is where Crowti, Tescrypt, Teerac, and Locky have been very active at.

We've also observed some malware authors providing a different method of distribution in the black market called ransom-as-a-service (RaaS). Malicious actors use RaaS to download the ransomware app builder and customize them accordingly. We've seen two threats, Sarento and Enrume, built through this type of service and deployed to infect machines during the second half of 2015.

How Samas is different from other ransomware?

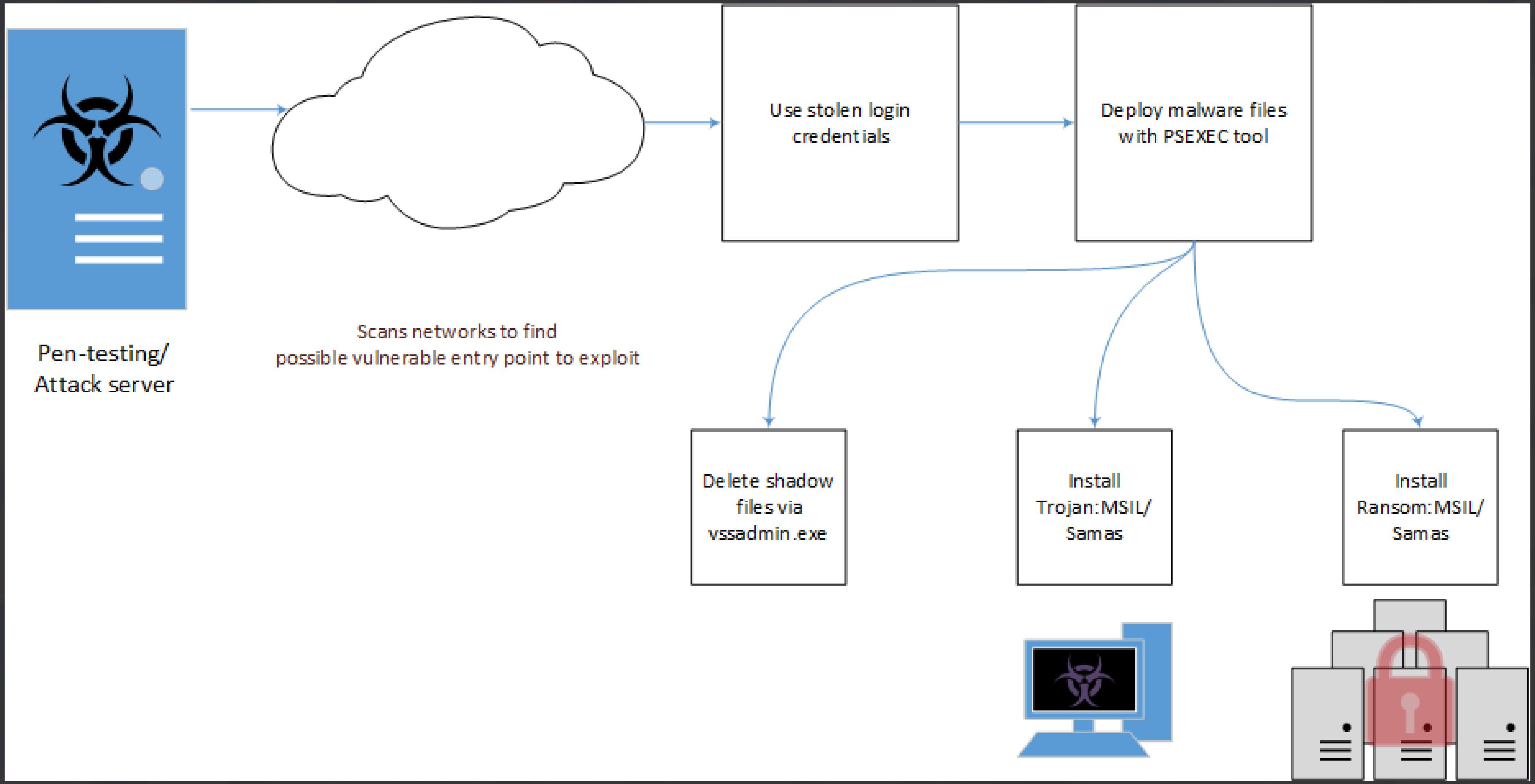
Ransom:MSIL/Samas, which surfaced in the past quarter, has a different way of getting into the system – it has a more targeted approach of getting installed. We have observed that this threat requires other tools or components to aid its deployment:

Pen-testing/
Attack server
Scans networks to find
possible vulnerable entry point to exploit
Use stolen login credentials
Deploy malware files with PSEXEC tool
Delete shadow files via vssadmin.exe
Install Trojan:MSIL/Samas
Install Ransom:MSIL/Samas

Figure 1: Ransom:MSIL/Samas infection chain

Source: https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/

Infection methods



Pen-testing/
Attack server
Scans networks to find
possible vulnerable entry point to exploit
Use stolen login credentials
Deploy malware files with PSEXEC tool
Delete shadow files via vssadmin.exe
Install Trojan:MSIL/ Samas
Install Ransom:MSIL/ Samas

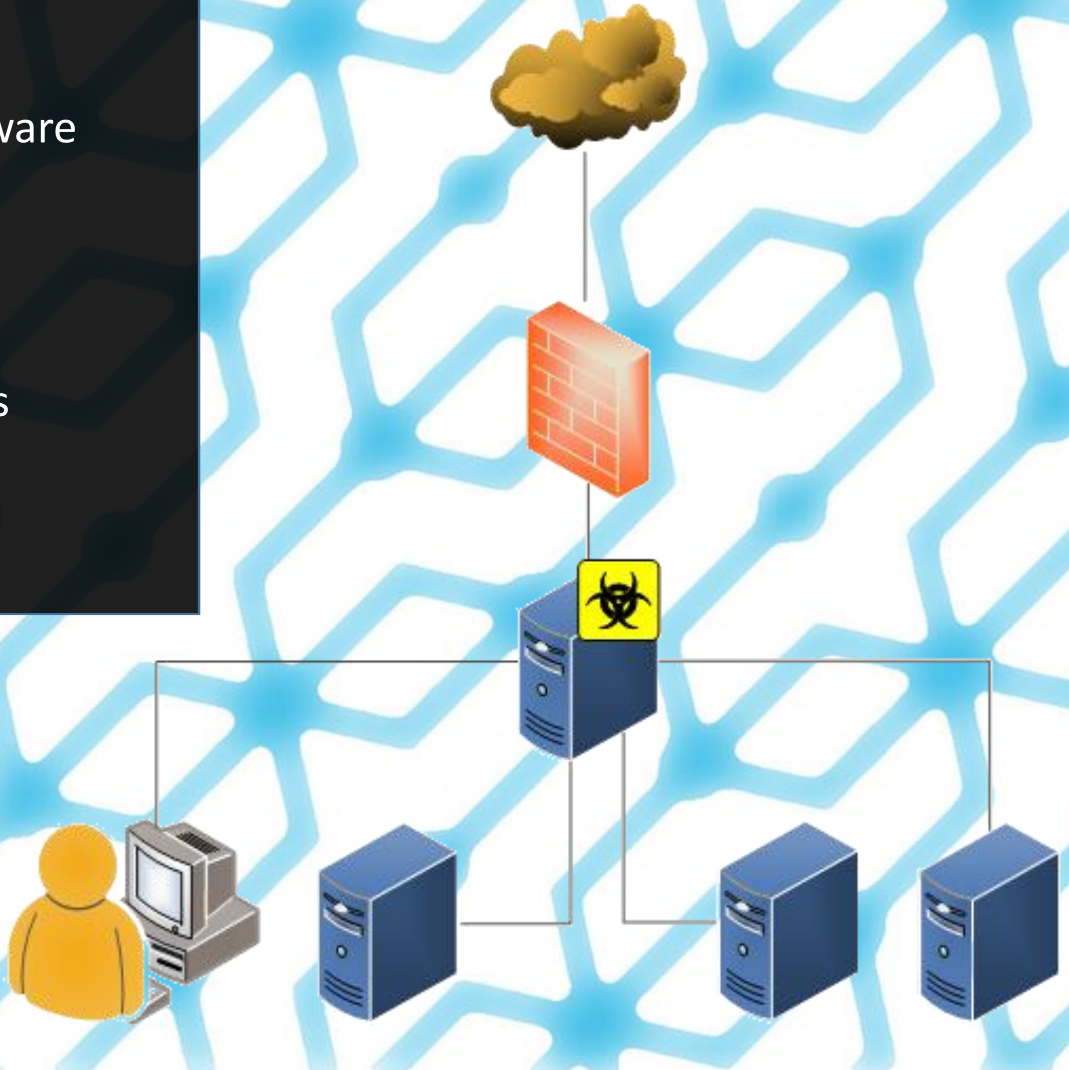
Source: https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/

Infection methods

⚠ Out of date/insecure software

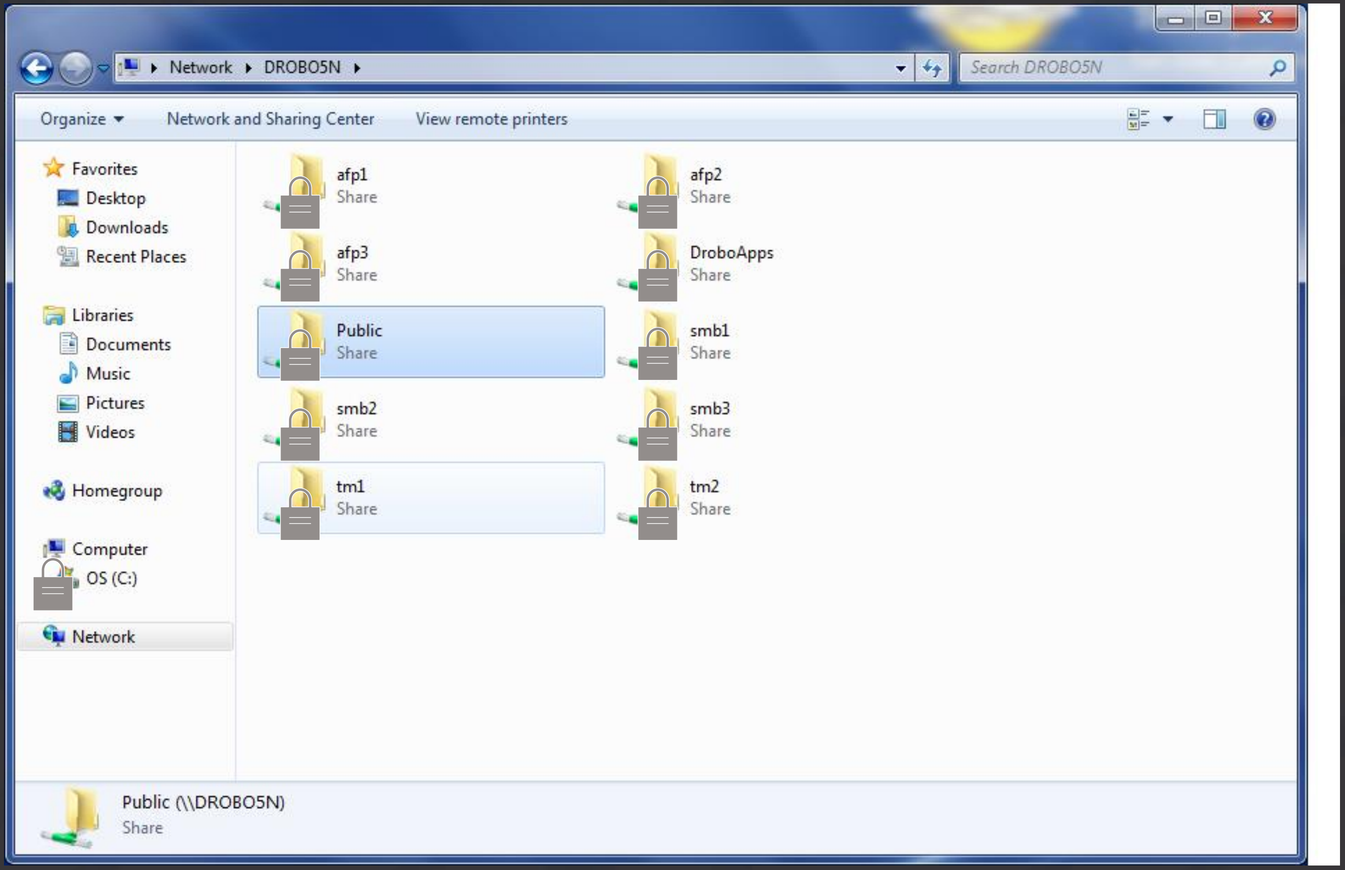
⚠ Default credentials

⚠ Lack of security awareness
by sysadmins



SYNDIS
Creative in Security

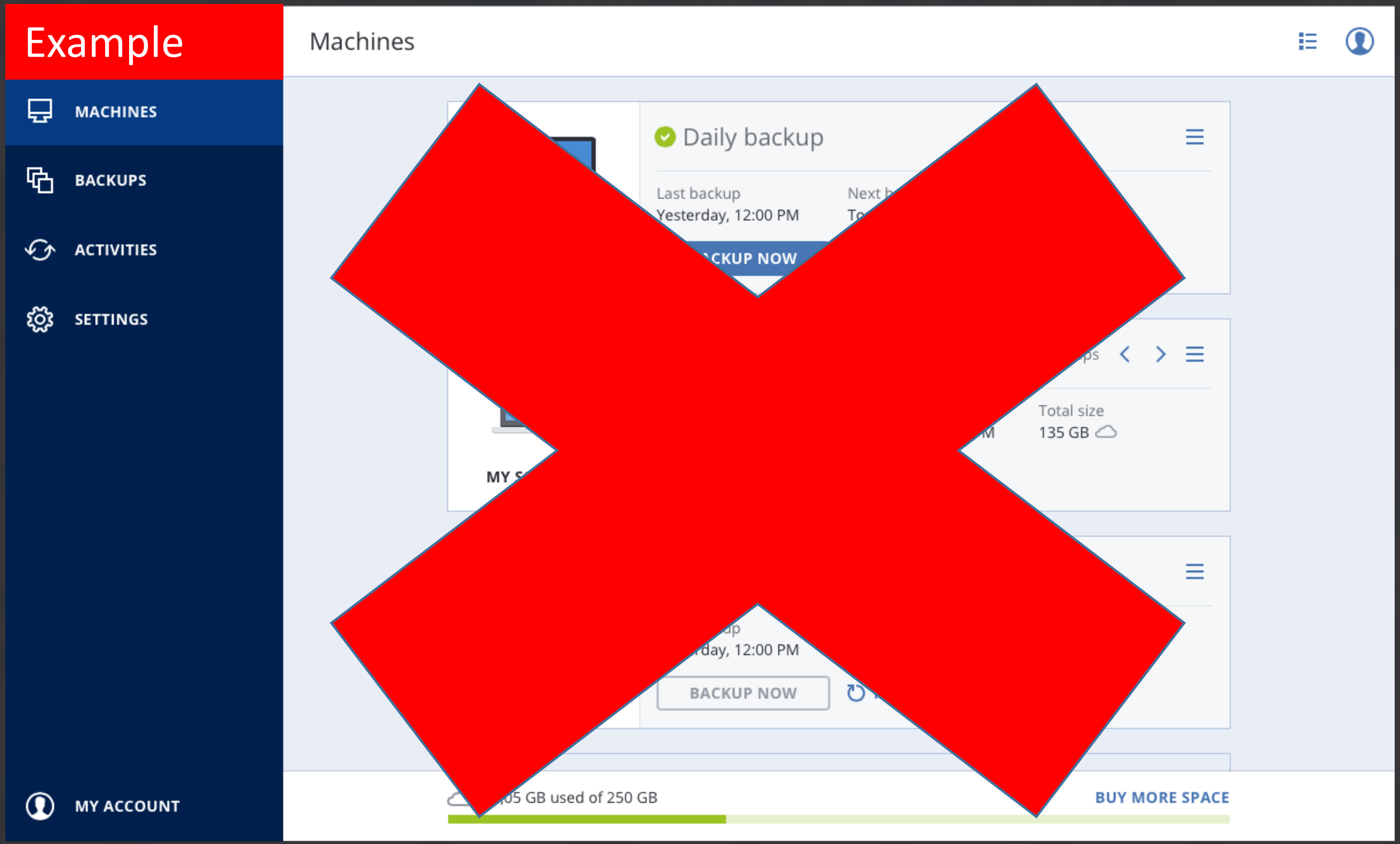
What happens next?



Source: https://dev-connecteddata.host4kb.com/admin/media_store/2/AA-01924/Win2.png

SYNDIS
Creative in Security

What happens next?



Daily backup

Last backup
Yesterday, 12:00 PM

Next b
To

Total size
135 GB

MY S

day, 12:00 PM

05 GB used of 250 GB

Source: http://www.acronis.com/en-us/blog/sites/default/files/acronis_backup_service_simplified_ui.png

SYNDIS
Creative in Security

Infected, what now?

Source: https://m.popkey.co/76b7ee/LmY5p.gif

Process

Source: https://media.giphy.com/media/A34x7CEKUkCyc/giphy.gif

SYNDIS
Creative in Security

Step 1 – Contain

Source: http://i.imgur.com/cpXMY96.gif

SYNDIS
Creative in Security

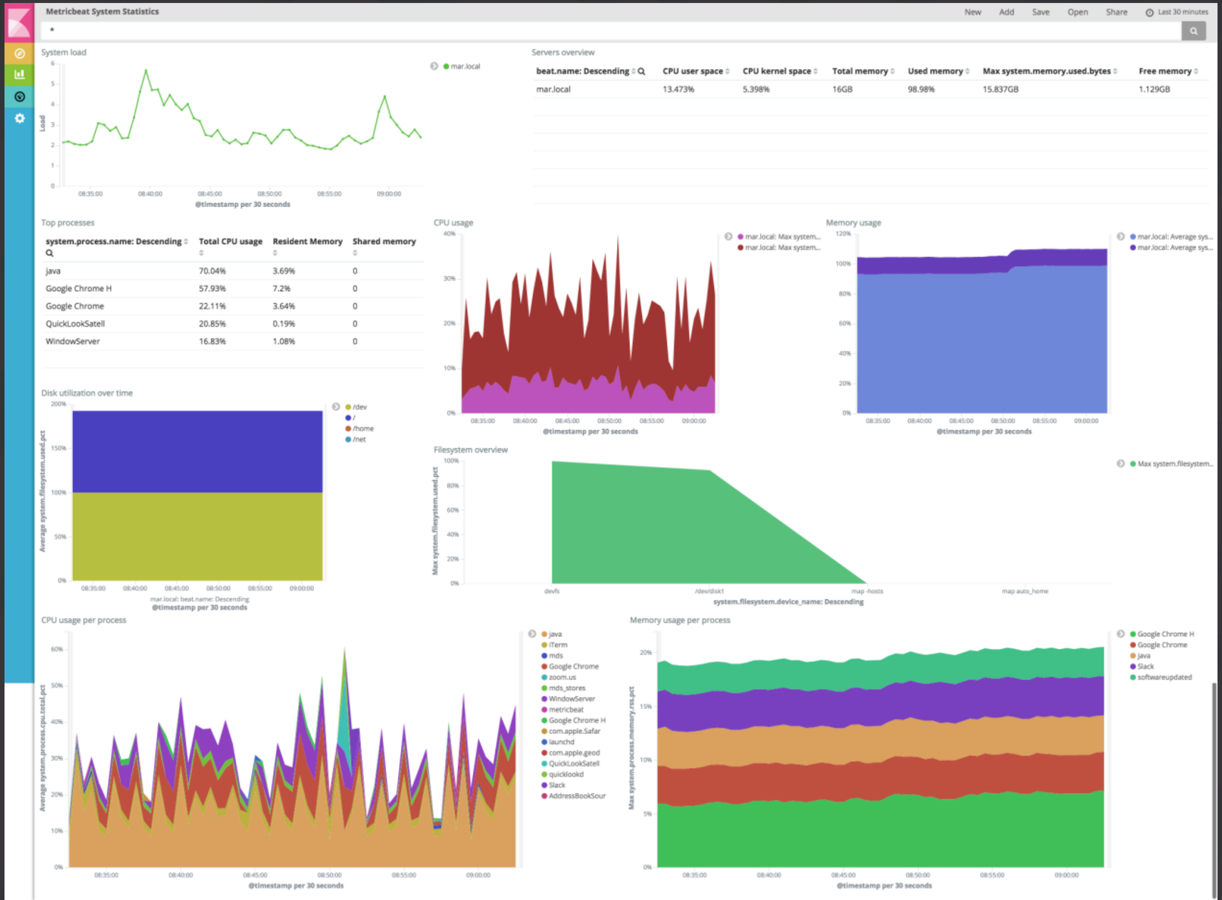
Step 1 – Contain

- Some ransomware will overwrite backups
  - Either directly
  - Or by changing the timestamp on files, thus invalidating differential backups
- Thus, don’t rely on backups. Do both differential, and full backups

Step 2 – Determine scope

- This often takes a while, and gets expensive with downtime
- Requires good logs
  - Netflow/network data
  - Event logs/AD logs/Sysmon
  - DNS Logs
- Ransomware will sometimes not change file ownership

Step 2 – Determine scope



Metricbeat System Statistics

Servers overview

beat.name: Descending	CPU user space	CPU kernel space	Total memory	Used memory	Max system.memory.used.bytes	Free memory
mar.local	13.473%	5.398%	16GB	98.98%	15.837GB	1.129GB

Top processes

system.process.name: Descending	Total CPU usage	Resident Memory	Shared memory
java	70.04%	3.69%	0
Google Chrome H	57.93%	7.2%	0
Google Chrome	22.11%	3.64%	0
QuickLookSatell	20.85%	0.19%	0
WindowServer	16.83%	1.08%	0

Source: https://www.elastic.co/guide/en/beats/metricbeat/current/images/metricbeat_system_dashboard.png

Step 3 - Recover

Source: http://33.media.tumblr.com/0b316f1e5a59cd5847e1ae1fdf09edc0/tumblr_mvnwki0c3d1qajc4eo1_r1_500.gif

SYNDIS
Creative in Security

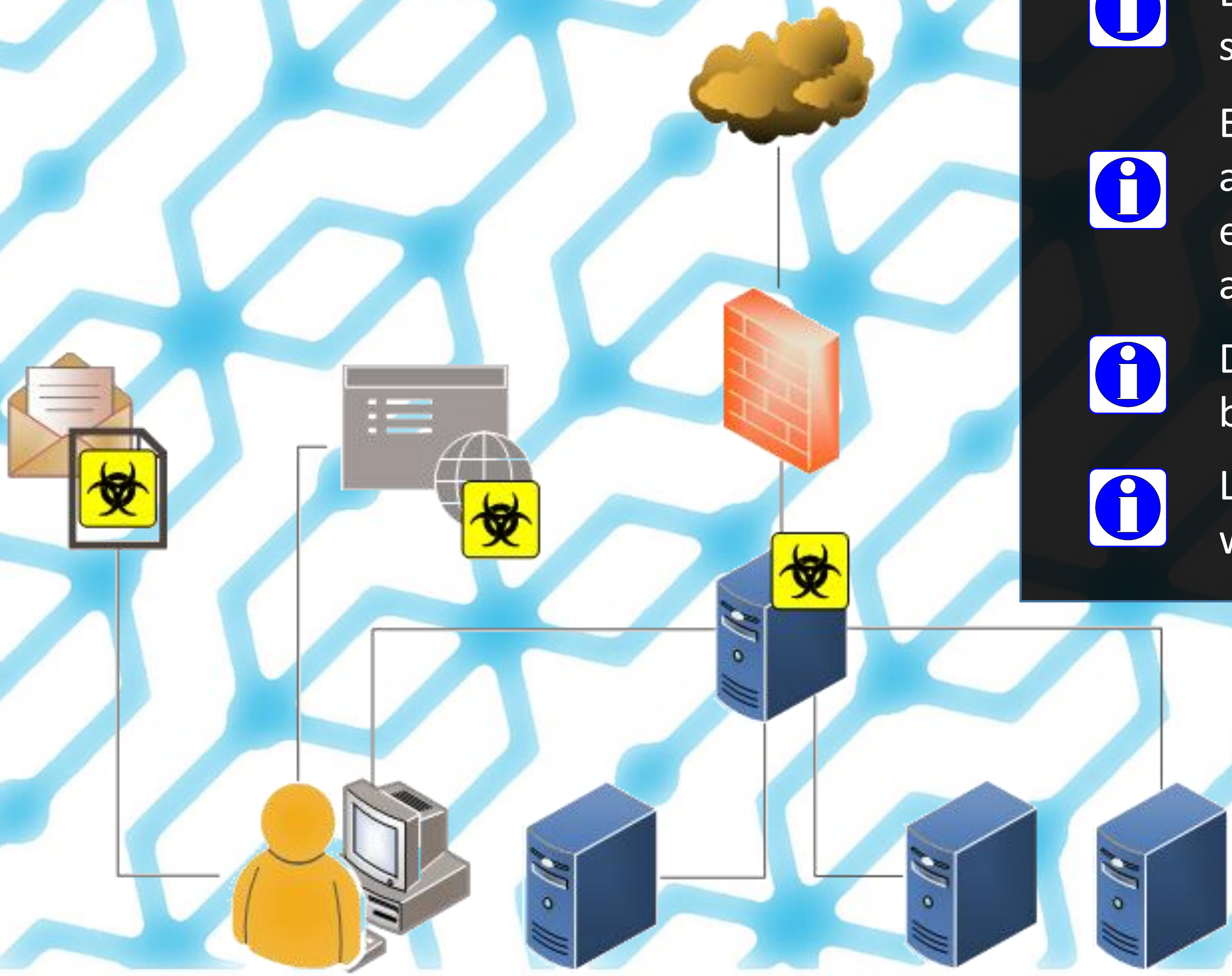
Step 3 - Recover

- Don’t attempt if you haven’t fully determined scope
- If your backups are intact, great. Restore!
- Sometimes paying is the only option

What to do?

Source: https://i.makeagif.com/media/4-23-2015/A1V4ZR.gif

Tips & tricks



- ℹ Ensure your software is up to date, and configured securely
- ℹ Ensure you have at least basic spam filter, antivirus
- ℹ Ensure you have security awareness, both by employees, and system admins
- ℹ Do both full, and differential backups
- ℹ Limit network share access where possible

Logging saves lives

Source: https://fsmedia.imgix.net/a5/15/8c/cc/11f3/4897/9d4d/e05daefe62d6/ride-logs-13gif.gif?w=700&auto=format&gifq=35

So what is your data worth?

Q&A

(if time allows)