

# Computer Security is Simple, The World is Not.

Raphaël Vinot and Quinn Norton

# Computer Security is Simple, The World is Not.

Raphaël Vinot and Quinn Norton



***To preserve anonymity and privacy,  
this talk will use screencaps of  
awkward stock photography to represent  
the real life stories we are sharing with you.***



# Syrian Arab Spring (2011-2012)







# DARKC

REMOTE ADMINISTRATION TOOL



# MET



[Home](#) » [Malware](#) » [DarkComet Surfaced in the Targeted Attacks in Syrian Conflict](#)

## DarkComet Surfaced in the Targeted Attacks in Syrian Conflict

Posted on: [February 23, 2012](#) at 7:24 pm    Posted in: [Malware](#)

Author: [Kevin Stevens and Nart Villeneuve](#) (Senior Threat Researchers)



The Internet has played a significant role in the [current conflict in Syria](#). The opposition has made increasing use of platforms such as *Facebook* to organize and spread their message. In response, supporters of the regime like the "[Syrian Electronic Army](#)" have sought to disrupt these activities by defacing websites and spamming *Facebook* pages. Recently, this conflict took on a new dimension with [reports](#) that suggested targeted malware attacks were being used against supporters of the Syrian opposition movement.

### ***Dark Comet RAT Used as "Syrian Spyware"***

The malware used in the attacks reportedly spreads through *Skype* chats. Once users execute the malware, it connects to a C&C (command and control) server in Syria at [{BLOCKED}](#).

[{BLOCKED}](#).0.28, which belongs to an IP range assigned to the *Syrian Telecommunications*

*Establishment*. While the malware has been described as "complex" and "invisible", it turns out that



Download from  
**Dreamstime.com**

This watermark-free image is for previewing purposes only.

40964780  
© Scott Griesel | Dreamstime.com







**“You should probably use Skype.”**

**“You should probably use Skype.”**

**“...I’m sorry we didn’t understand, or help.”**

# **The Principles We Want You to Leave With**

- **Listen to your users, they know their environment better than you do**

**Listening to your users mean shutting up.  
Even if it's painful.  
Especially when it's painful,  
and you know they're technically incorrect  
and  
it's driving you crazy.**







## NEWS



## Malvertising: Daily Mail ads 'briefly linked' to malware

🕒 16 October 2015 | Technology



THINKSTOCK

Readers of the Daily Mail's website were shown fake advertisements that linked to malware, according to a security company.




## Security

# You've been Drugged! Malware-squirting ads appear on websites with 100+ million visitors

eBay, Drudge Report, etc inadvertantly carry evil adverts

By Shaun Nichols in San Francisco 14 Aug 2015 at 22:45

54 

SHARE ▼

Search



ked' to malware



THINKSTOCK

Readers of the Daily Mail's website were shown fake advertisements that linked to malware, according to a security company.

Security

You've been Drugged  
squirting ads at  
100+ million visitors

eBay, Drudge Report,  
adverts

By Shaun Nichols in San Francisco



Read  
malware

Forbes / Tech / #GettingBuzz

MAR 2, 2017 @ 09:00 AM

4,630



EDITOR'S PICK

12 Stocks to Buy Now

## In Fake News Era, Facebook Still Struggling With Bogus Ads



**Matt Drange**, FORBES STAFF ✓

*I cover Donald Trump's business dealings. Get in touch.*

[FULL BIO](#) ✓



*Facebook CEO Mark Zuckerberg speaks at the company's annual*

You've been Drugged  
squirting ads at  
100+ million visi

Forbes / Tech / #GettingBuzz

eBay. Drudge Report.

adv



By Sh

Products

Services

Solutions

Partners

Now

# Malware With Your News? Forbes Website Victim of Malvertising Attack

September 22, 2015 | by J. Gomez, Genwei Jiang | Threat Research



From Sept. 8 to Sept. 15, 2015, the Forbes.com website was serving content from a third-party advertising service that had been manipulated to redirect viewers to the Neutrino and Angler exploit kits. We notified Forbes, who worked quickly to correct the issue.



Facebook CEO Mark Zuckerberg speaks at the company's annual

Reade  
malwa



Security

You've been Drudged  
squirting ads at  
100+ million visi

Forbes / Tech / #GettingBuzz

eBay. Drudge Report.  
adv



By Sh

Products

Services

Solutions

Partners

Now

Malware  
Webs



REVIEWS

NEWS

VIDEO

HOW TO

SMART HOME

CARS

DEALS

DOWNLOAD

September 22, 20



SECURITY

# Drudge Report accused of serving malware, again

Drudge says a Senate committee has falsely accused the conservative news aggregation site of spreading malware, but a CNET reader says it's true.

BY ELINOR MILLS / MARCH 9, 2010 9:31 AM PST



Re  
ma

Facebook CEO Mark Zuckerberg speaks at the company's annual

Security

You've  
squir  
100+

eBay. I  
adv

By Sh

# Malvertising campaign hits MSN.com, NY Times, BBC, AOL

Now

[Understanding Pulse Wave DDoS Attacks Free White Paper Download](#)

LOAD

In the last couple of days, visitors of a number of highly popular websites have been targeted with malicious adverts that attempted to install malware (mostly ransomware, but also various Trojans) on their systems.

he  
are, but



Finder

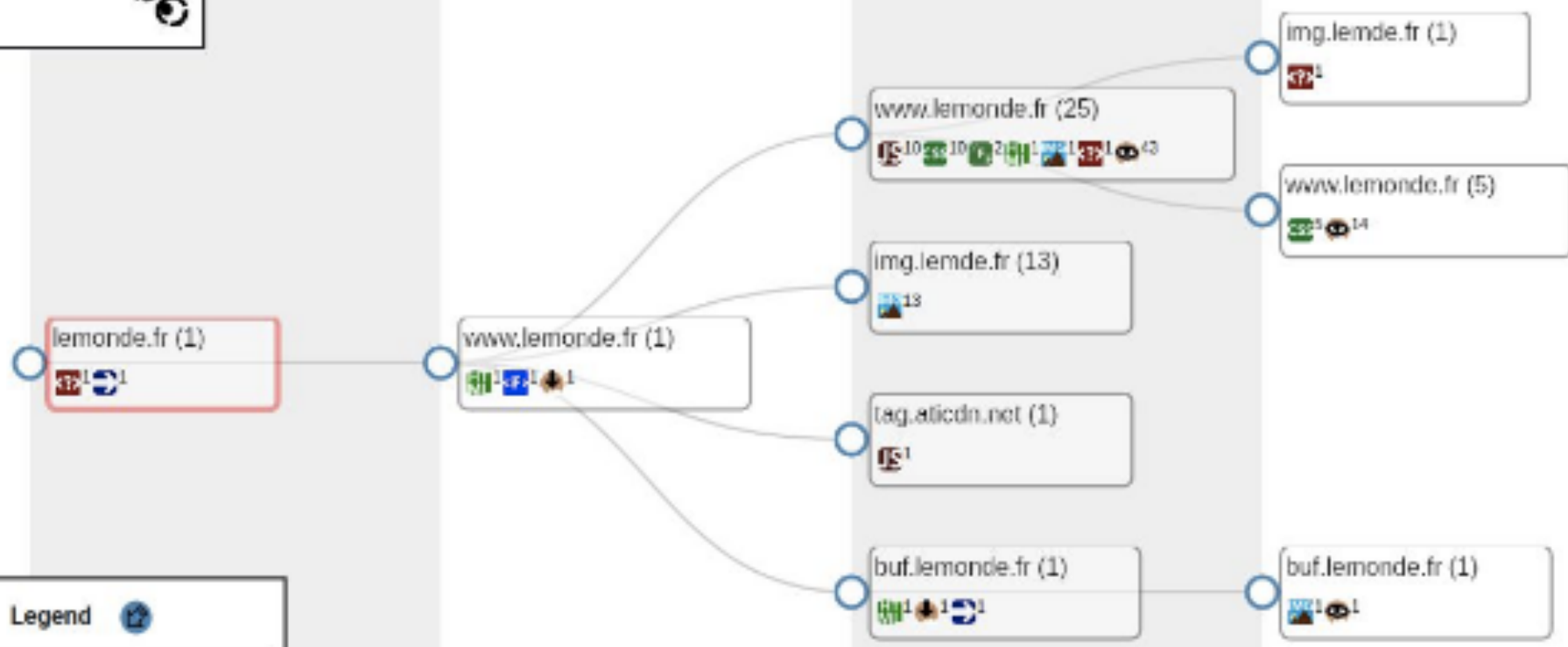
# Malvertising

*Facebook CEO Mark Zuckerberg speaks at the company's annual*

**“How can we know what’s on our site?”**

lookyloo

Lookyloo



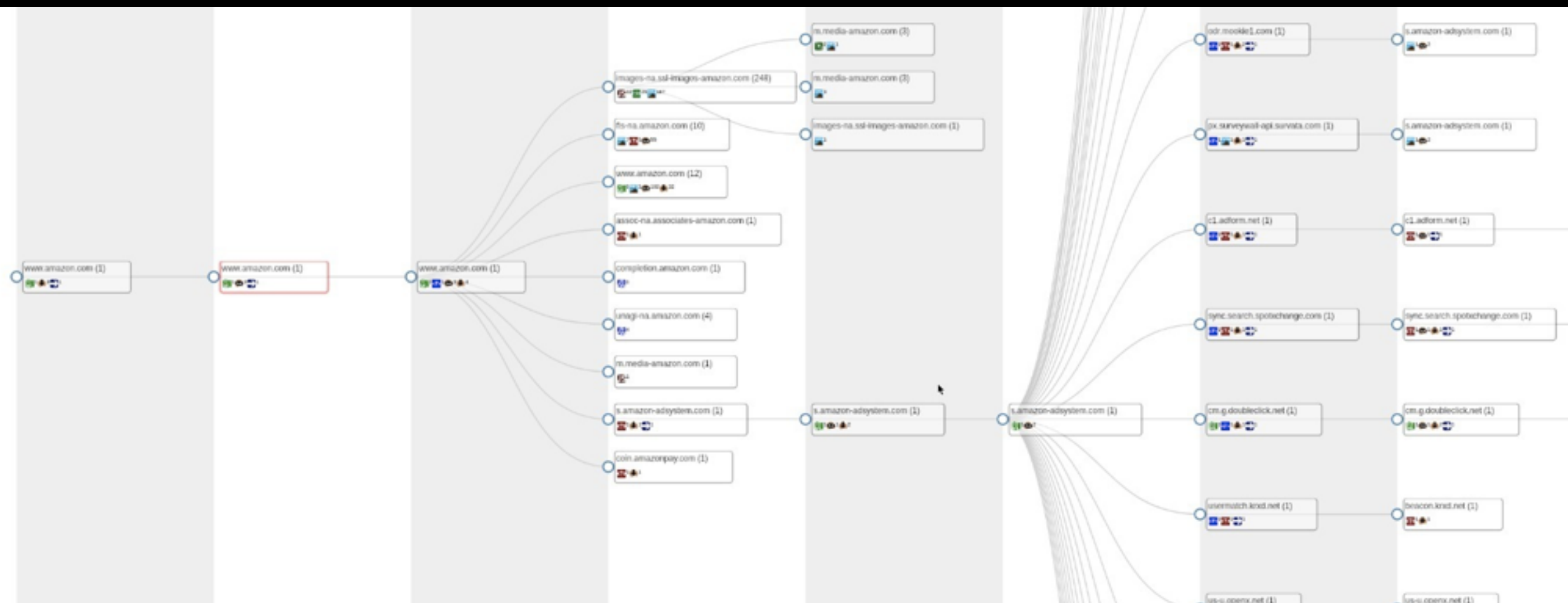
Legend

- Javascript
- Cookie received
- Cookie read
- Redirect
- Font
- HTML
- JSON
- CSS
- EXE
- Image
- Video
- iFrame
- Content type not set/unknown

Tree details

Root URL: http://lemonde.fr/  
Start time: 2019-07-01T14:40:14.100265  
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36  
Os: Win10  
Browser: Chrome Generic  
Screenshot: [Download](#) [View](#)





Lookyloo



#### Legend

- JavaScript
- Cookie received
- Cookie read
- Redirect
- Font
- HTML
- JSON
- CSS
- EXE
- Image
- Video
- iFrame
- Content type not set/unknown

SPURKESS

Login

FR DE GB

LUXTRUST

User ID:

Password:

Annuler S'authentifier

Token

Tree details

Root URL: [http://cutt.ly/mw/0000](#)

Start time: 2019-11-21T09:32:01.481478

User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36

Os: Win10

Browser: Chrome 74.0

Screenshot [Download](#) [Hide](#)



# **The Principles We Want You to Leave With**

- **Listen to your users, they know their environment better than you do**
- **If you don't listen to your users, you don't know how to do your job**

**Take notes,  
very possibly on paper.  
You will need them.**

# Lessons Learned from Training Company Staff in Luxembourg





This web page is blocked by administrator..



© Blockit 2010

[Change settings](#)



## **Consensus Policy Resource Community**

available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

### **3.3 Internet Use Filtering System**

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for <Company Name>'s corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email



### **3.4 Internet Use Filtering Rule Changes**

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.



# FilePizza


Free peer-to-peer file transfers in your browser.

We never store anything. Files only served fresh.

[select a file](#)

BTC Donations: 1P7yFQAC3Empvs87K9s6bKpVxEP1LPoQnY


Cooked up by [Alex Kern](#) & [Neeraj Baid](#) while eating [Sliver](#) @ UC Berkeley · [FAQ](#) · [Fork us](#)

 **GigaTribe**  
Share in Confidence

Sign In Sign Up

Home Software Prices Help Private Space

Blog Facebook GigaTribeHub API



Private, Secure, Unlimited  
File Sharing Software

[Free download](#)

No  
Special  
Adware  
Malware...

### How it works

1

Install  
Download GigaTribe,  
and create an account


2

Invite  
Invite People  
You Rely On


3

Share  
Select the folders  
you want to share

### Secure & Confidential



- Your files remain on your computer. GigaTribe does not host any file.
- You decide who join in your private network.
- Files transferred are protected by the secrecy of correspondence.
- Downloads are encrypted (Blowfish 256-bit).
- GigaTribe is 100% legal.
- GigaTribe is following the Federal Trade Commission [Best Practices to Protect Users Against Inadvertent File Sharing](#).



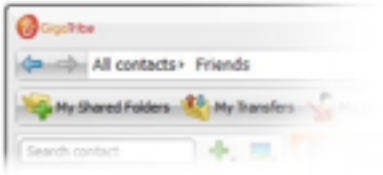
### Why use GigaTribe

- Share **large files** with NO limitations on file quantity or size.
- Files are available in their original format.
- You don't waste time uploading files.
- Your files remain under your control.
- It's a two-way sharing service.
- CNET editor's rating: ★★★★★


[More information...](#)

### News

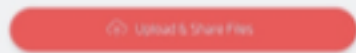
Today ~ 8:58 pm  
**1,741,130 user accounts created!**



Search contact


files.fm  Upload files Features and pricing


## Store, Share and Sell Files





it's only a few lines


Create free account and check other apps

 Store

 Sell

 Publish

 Backup

 Receive

1TB = 88€

LIFETIME STORAGE

10 year

2013-2023

[Buy your private cloud](#)

file sharing



Search

You found 305 file sharing website templates from \$3. All created by our Global Community of independent Web Designers and Developers.

× Filter & Refine

All prices are in USD



Best match

Best sellers

Newest

Best rated

Trending

Price

Category



305 items

Term 'file sharing' ×

[Clear all](#)

All categories

305

PSD Templates

88

WordPress

85

Site Templates

70

Blogging

23

Static Site Generators

12

Sketch Templates

9

Marketing

7

Courses

5

Muse Templates

4

CMS Themes

2

Tags



☐ Blog

100

☐ Clean

97

☐ Modern

82

☐ Responsive

80

☐ Minimal

66

☐ Creative

62

☐ Portfolio

62

Price



\$3

\$75



Sales



Cloud Services and Hosting WP Theme



Tags: agency, business, clean, cloud storage, company, cor... See all tags

**CloudMe | Cloud Storage & File-Sharing Services Word...**  
by AncoraThemes in Technology

- Cloud Storage, **File-Sharing** Services WP Theme
- 4 cloud storage, **file-sharing** services homes
- wpbakery+extensions bundle, wpml, revolution



\$59

★★★★★ (4)

307 Sales

Last updated: 4 Sep 19

Preview



Tags: activity, bbpress, buddypress, calendar, community, ... See all tags

**LaraUpload - File Sharing PSD Template**  
by Ra-Themes in Miscellaneous

- Awesome & Modern Design
- Fully customizable
- Well organized layers

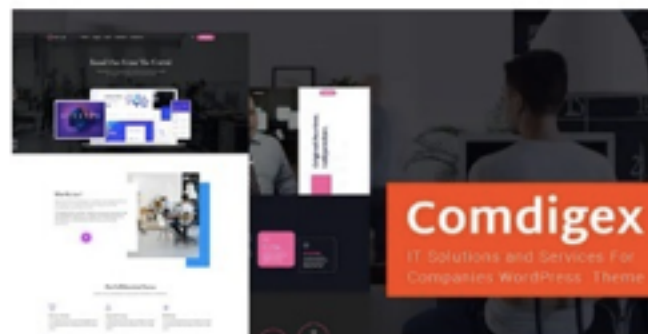


\$10

2 Sales

Last updated: 28 Aug 18

Add To Cart



Tags: Apple Mac Repair, Computer Printer Services, Mana... See all tags

**Comdigex - IT Solutions and Services Company WP Th...**  
by Mymoun in Technology

- Perfect for any service related business
- One-Click installer, get a website in minutes
- RTL, GDPR Ready



\$49

16 Sales

Last updated: 4 Oct 19

Preview





luxembourg



## FILES 20 / 2.29 K

bbc108aa169554450aae36c5026fbb5f84f08d46a2857df302312e80e1db863f



com.simplmobiletools.calendar

android

apk



3530d53ec34fc33a7a85fb3b9b6558de6ad9cb7c39f35555d4eee3633b108bc7



com.simplmobiletools.calendar.pro

android

apk



ceab47f25477459e65910be52d7269764c04a3c96ebcb7a5bcbca48f275a2e39



/rethinkingdistribution/docs/pwc-publ-ideal-fund.pdf



pdf

autoaction



36b821c739f6f6327a659b6f418c3276b5fc14a371bb3ad464a484f9bc8df9aa



/rethinkingdistribution/docs/rethinking-distribution.pdf



pdf



7fd0067a8c689fccf6ea52b7f95537750481747d80fc87f73cca02ba56ec46f8



JCam-windows-installer.exe



peexe

signed

overlay

runtime-modules



b765c387b9104e1568d76624de6cdb0287561345a39096a78a7836603497e3c1



eu.mobile.icard



android

apk

runtime-modules

reflection

contains-elf



024e4dfe55022accb8dd5fa110c1955b3f445bf02cb2c2cfca50d439a9f284d3



...20(Luxembourg)%20S.A.%20-%20Current%20P%20&%20I%20Challenges.pdf



pdf



cc63352e22fa067bb502aa7d20ae5a2f1a96a16c3cd36ff4b194e35a827633f7



com.nyxcore.genlang

android

apk



d344f42d3ea8049b8b54bd1849c4e650818f503609004c1c61b8ba4bf74d9af0



luxembourg\_1910.zip



zip









# **The Principles We Want You to Leave With**

- **Listen to your users, they know their environment better than you do**
- **If you don't listen to your users, you don't know how to do your job**
- **If you don't listen to your users, you won't understand their jobs**

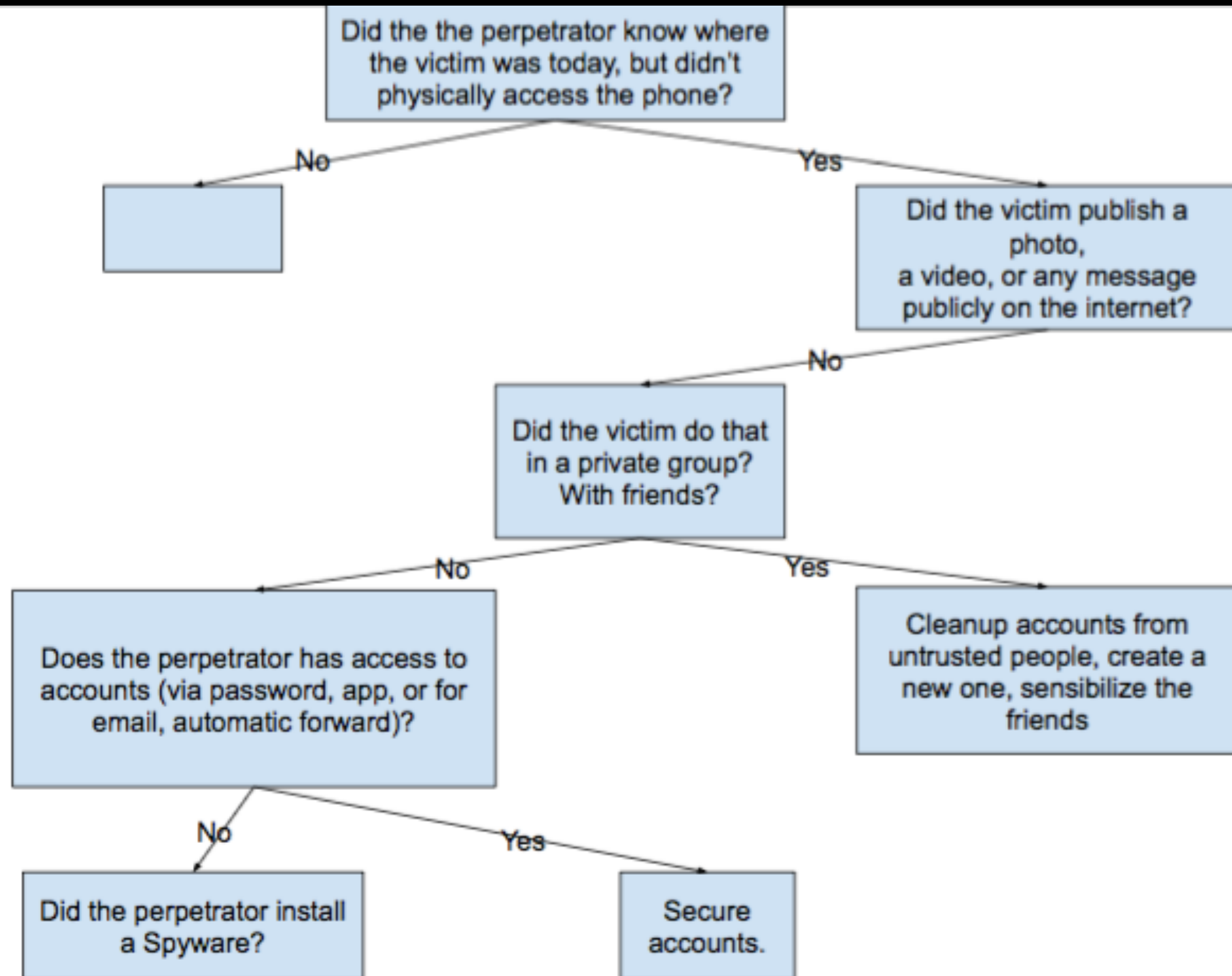
# Get Out of Your Office



# Supporting Domestic Violence Survivors









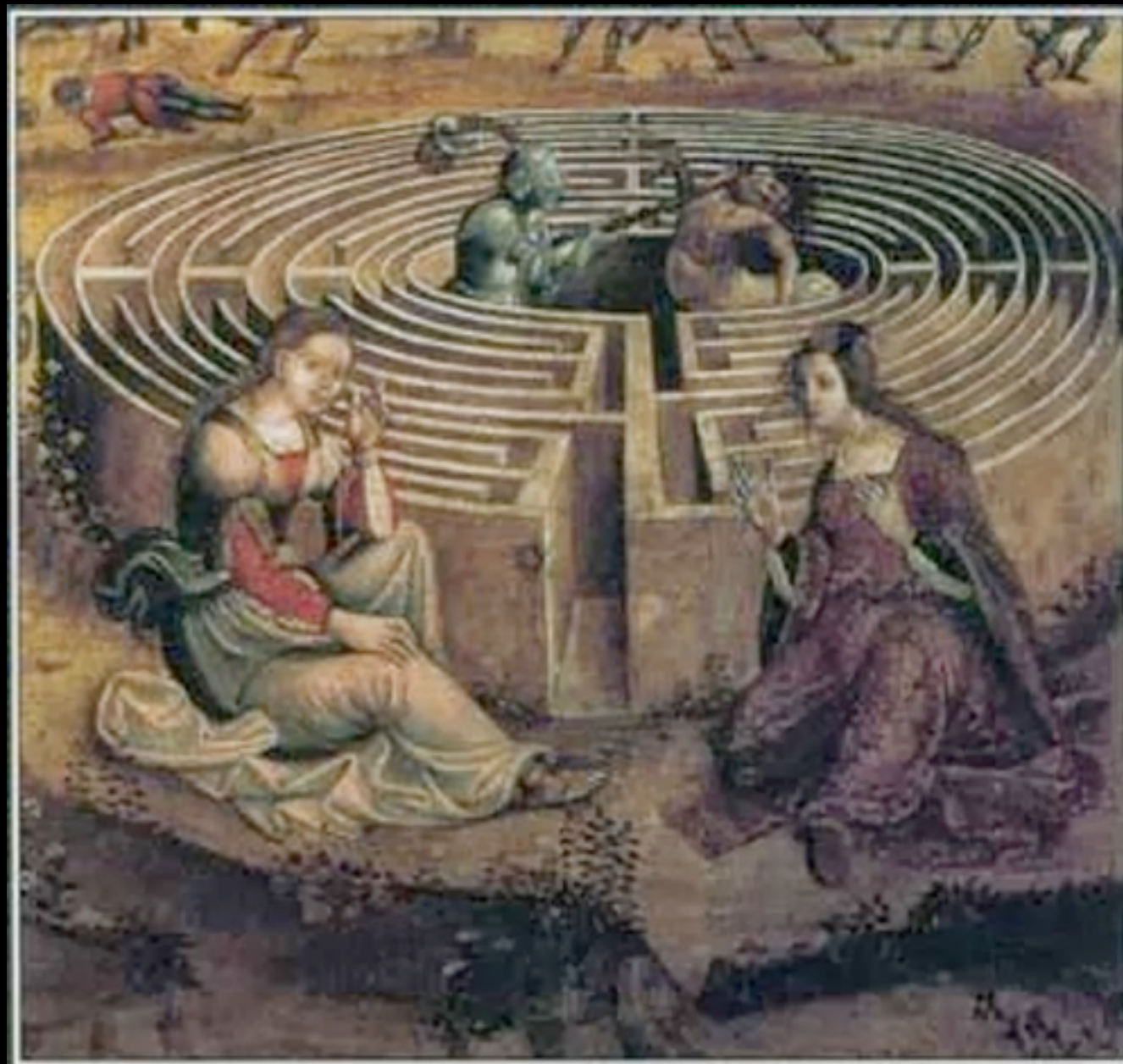


# **The Principles We Want You to Leave With**

- Listen to your users, they know their environment better than you do**
- If you don't listen to your users, you don't know how to do your job**
- If you don't listen to your users, you won't understand their jobs**
- You can't ever be sure, but the closer you work with your users the more you can all understand the risks.**

# Your Users Create Useful Mythology

*“All things are true, even false things.”*



**When you're explaining:**

**Don't tell your user what to do; tell them what  
it's doing**

**Arrive at the right answer together.**

**Extend their metaphors whenever you can, but  
gently.**

**Offer to go into technical details... but only if  
they want to.**













[www.shutterstock.com](http://www.shutterstock.com) • 141968254



**Don't scare your users,  
and don't let fear  
destroy your relationship with them.**



# **The Principles We Want You to Leave With**

- Listen to your users, they know their environment better than you do**
- If you don't listen to your users, you don't know how to do your job**
- If you don't listen to your users, you won't understand their jobs**
- You can't ever be sure, but the closer you work with your users the more you can all understand the risks.**
- Fear can undo all the other good things on this list.**



**Thanks!**

**If you need us to listen to you:  
(not on Skype, sorry)**

**@rafi0t - Raphaël Vinot  
raphael.vinot@circl.lu**

**@quinnnorton - Quinn Norton  
quinn@quinnnorton.com**