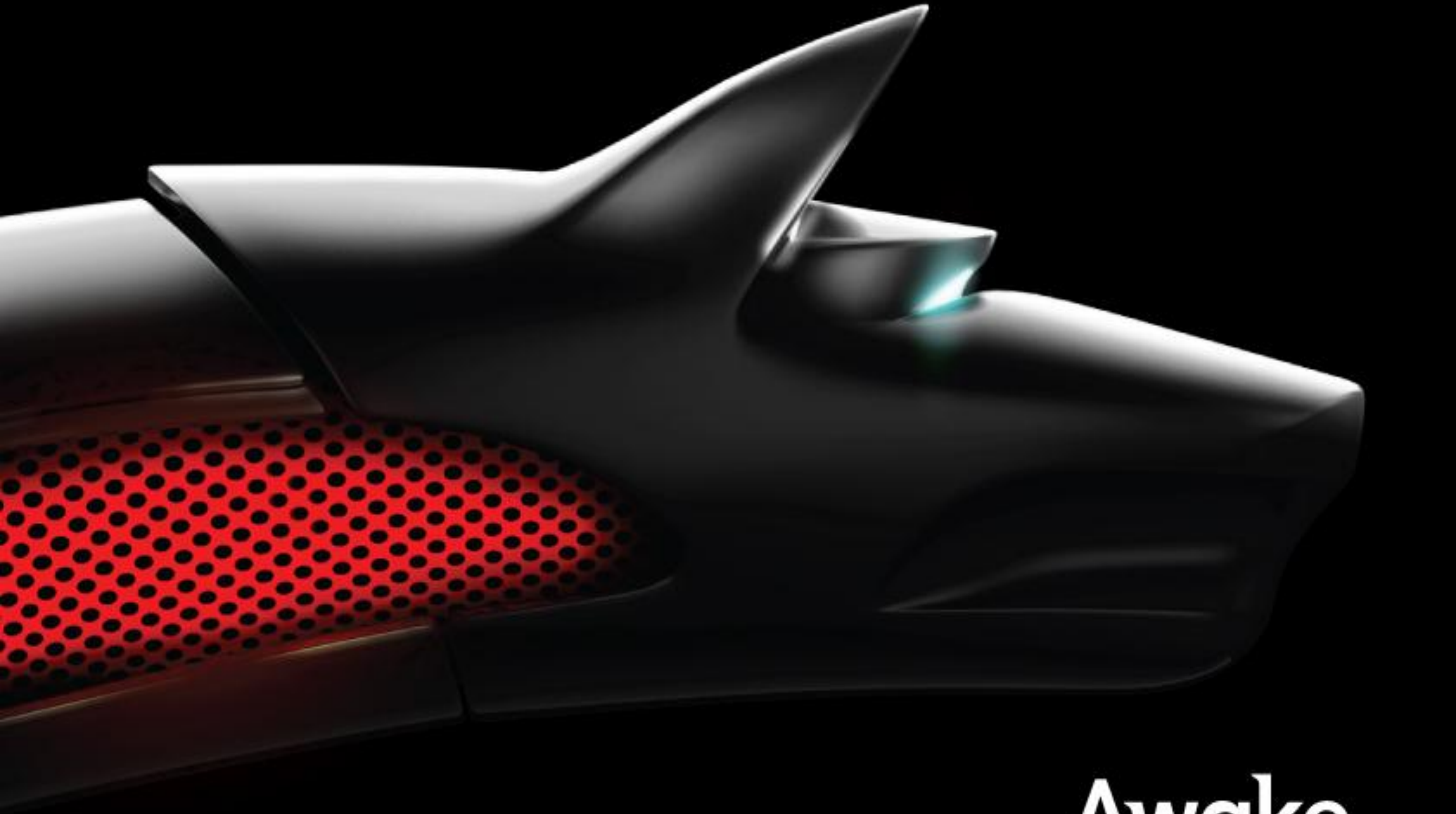


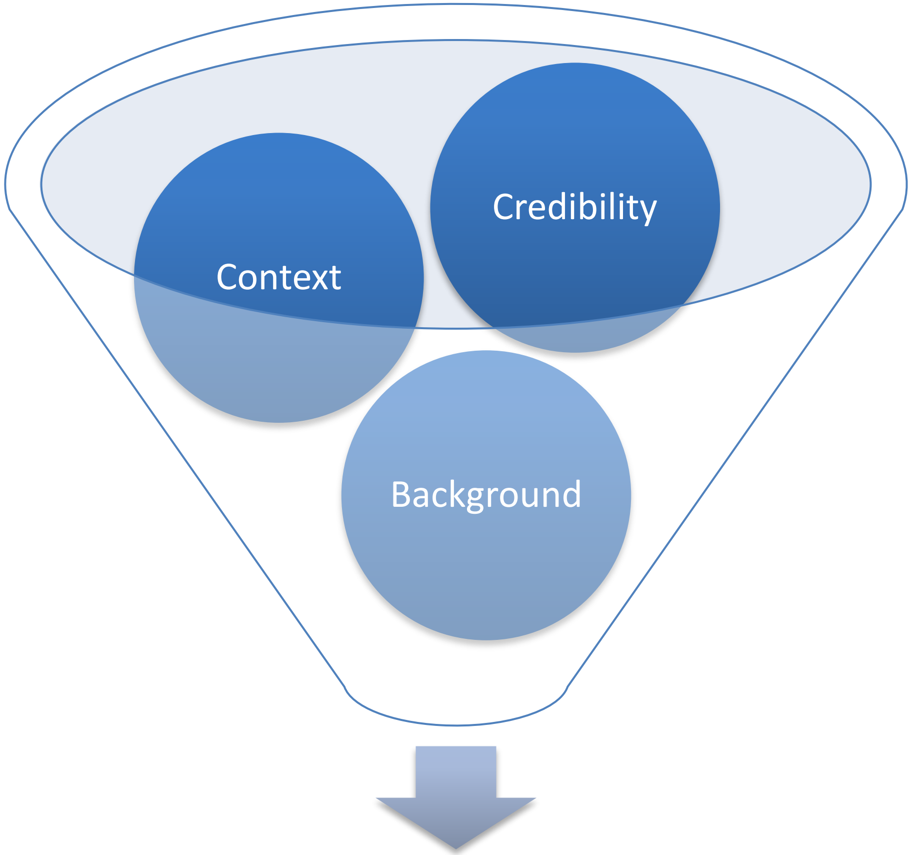
Awake

Automating Social Engineering

Alexandru Catalin Cosoi – Head of Online Threats Lab

Daniel Dichiu – NLPT Researcher

Social Engineering



The clever manipulation of the natural human tendency to trust.

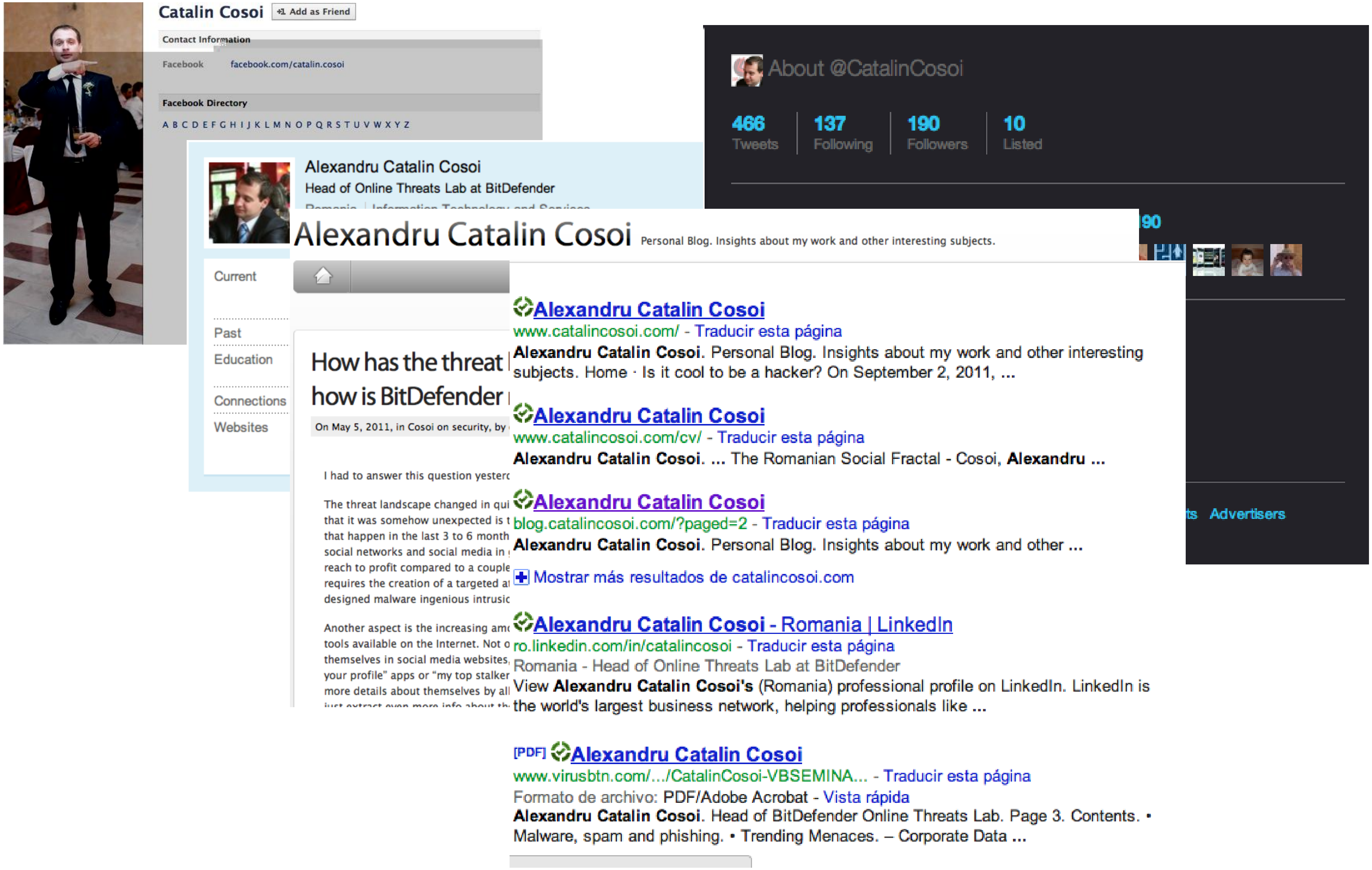
Copyright@bitdefender 2011 / www.bitdefender.com

Questions that need to be asked

1. What is your name or nickname?
2. What are your interests?
3. Who do you work for?
4. Who are your friends/colleagues?
5. What is you job title?
6. Who is you manager/CEO/director?
7. Who are your family members?
8. Are you married? With whom?
9. Do you have any kids? What are their names?
10. Where do you live? Where were you born?
11. How much do you earn?
12. Where do you stay? How expensive is your house?

Copyright@bitdefender 2011 / www.bitdefender.com

Our online identity



Catalin Cosoi
+1 Add as Friend
Contact Information
Facebook
facebook.com/catalin.cosoi
Facebook Directory
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alexandru Catalin Cosoi
Head of Online Threats Lab at BitDefender

Alexandru Catalin Cosoi Personal Blog. Insights about my work and other interesting subjects.

How has the threat
how is BitDefender

On May 5, 2011, in Cosoi on security, by

I had to answer this question yesterc

The threat landscape changed in qui
that it was somehow unexpected is t
that happen in the last 3 to 6 month
social networks and social media in
reach to profit compared to a couple
requires the creation of a targeted a
designed malware ingenious intrusic

Another aspect is the increasing am
tools available on the Internet. Not o
themselves in social media websites
your profile" apps or "my top stalker
more details about themselves by all

Alexandru Catalin Cosoi
www.catalincosoi.com/ - Traducir esta página
Alexandru Catalin Cosoi. Personal Blog. Insights about my work and other interesting subjects. Home · Is it cool to be a hacker? On September 2, 2011, ...

Alexandru Catalin Cosoi
www.catalincosoi.com/cv/ - Traducir esta página
Alexandru Catalin Cosoi. ... The Romanian Social Fractal - Cosoi, **Alexandru** ...

Alexandru Catalin Cosoi
blog.catalincosoi.com/?paged=2 - Traducir esta página
Alexandru Catalin Cosoi. Personal Blog. Insights about my work and other ...

Mostrar más resultados de catalincosoi.com

Alexandru Catalin Cosoi - Romania | LinkedIn
ro.linkedin.com/in/catalincosoi - Traducir esta página
Romania - Head of Online Threats Lab at BitDefender
View **Alexandru Catalin Cosoi's** (Romania) professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like ...

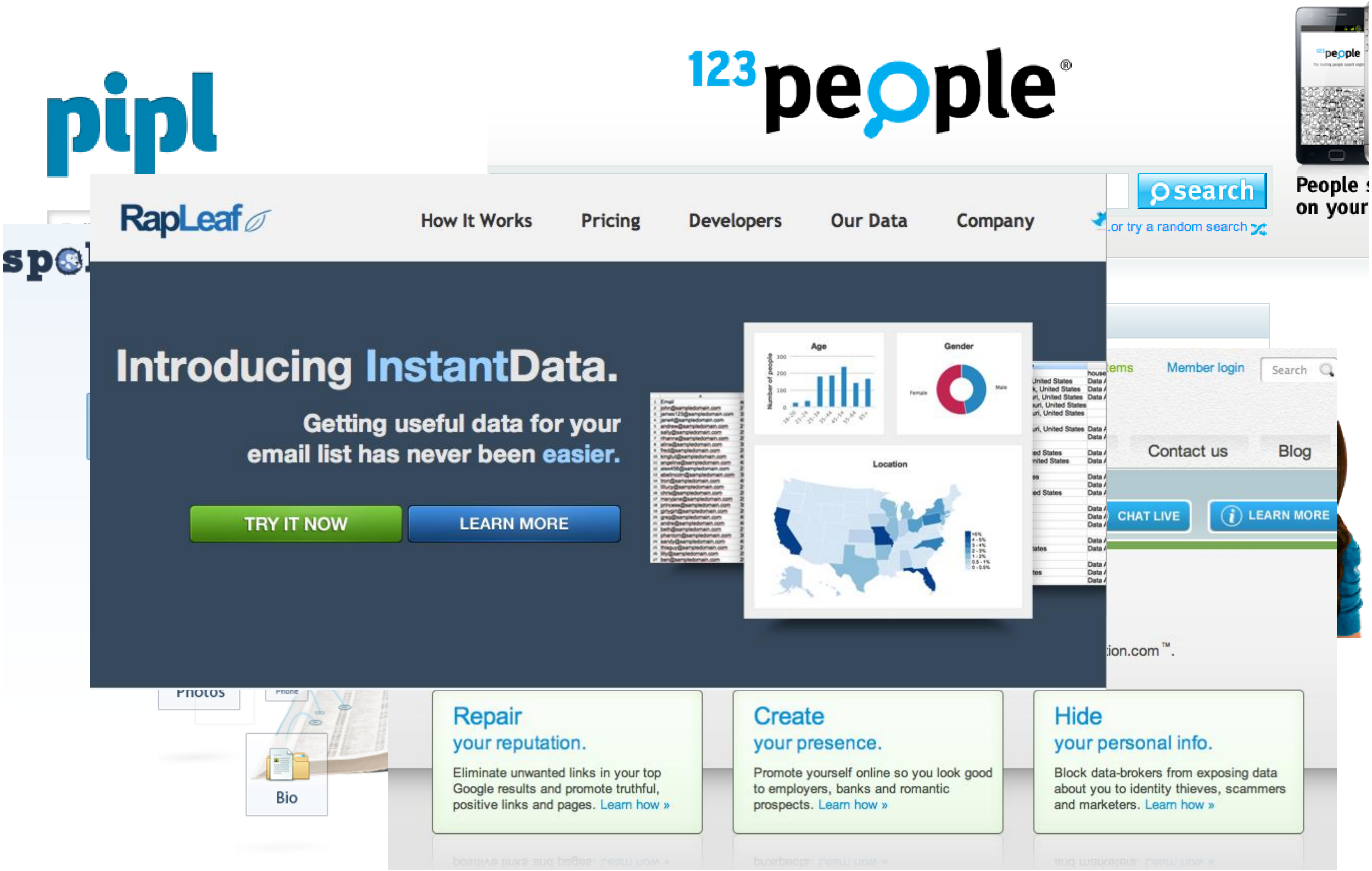
[PDF] **Alexandru Catalin Cosoi**
www.virusbtn.com/.../CatalinCosoi-VBSEMINA... - Traducir esta página
Formato de archivo: PDF/Adobe Acrobat - Vista rápida
Alexandru Catalin Cosoi. Head of BitDefender Online Threats Lab. Page 3. Contents. • Malware, spam and phishing. • Trending Menaces. – Corporate Data ...

Copyright@bitdefender 2011 / www.bitdefender.com

Stats

- 24% of Safego users found something malicious posted on their wall
- 90% of malicious Facebook apps were designed to access profile information
- 20% of Android malware discovered so far was designed for phishing or for immediate profit
- 80% of Android malware was designed to extract information from the device

Tools



Introducing InstantData.

Getting useful data for your email list has never been easier.

Repair your reputation.

Eliminate unwanted links in your top Google results and promote truthful, positive links and pages. Learn how »

Create your presence.

Promote yourself online so you look good to employers, banks and romantic prospects. Learn how »

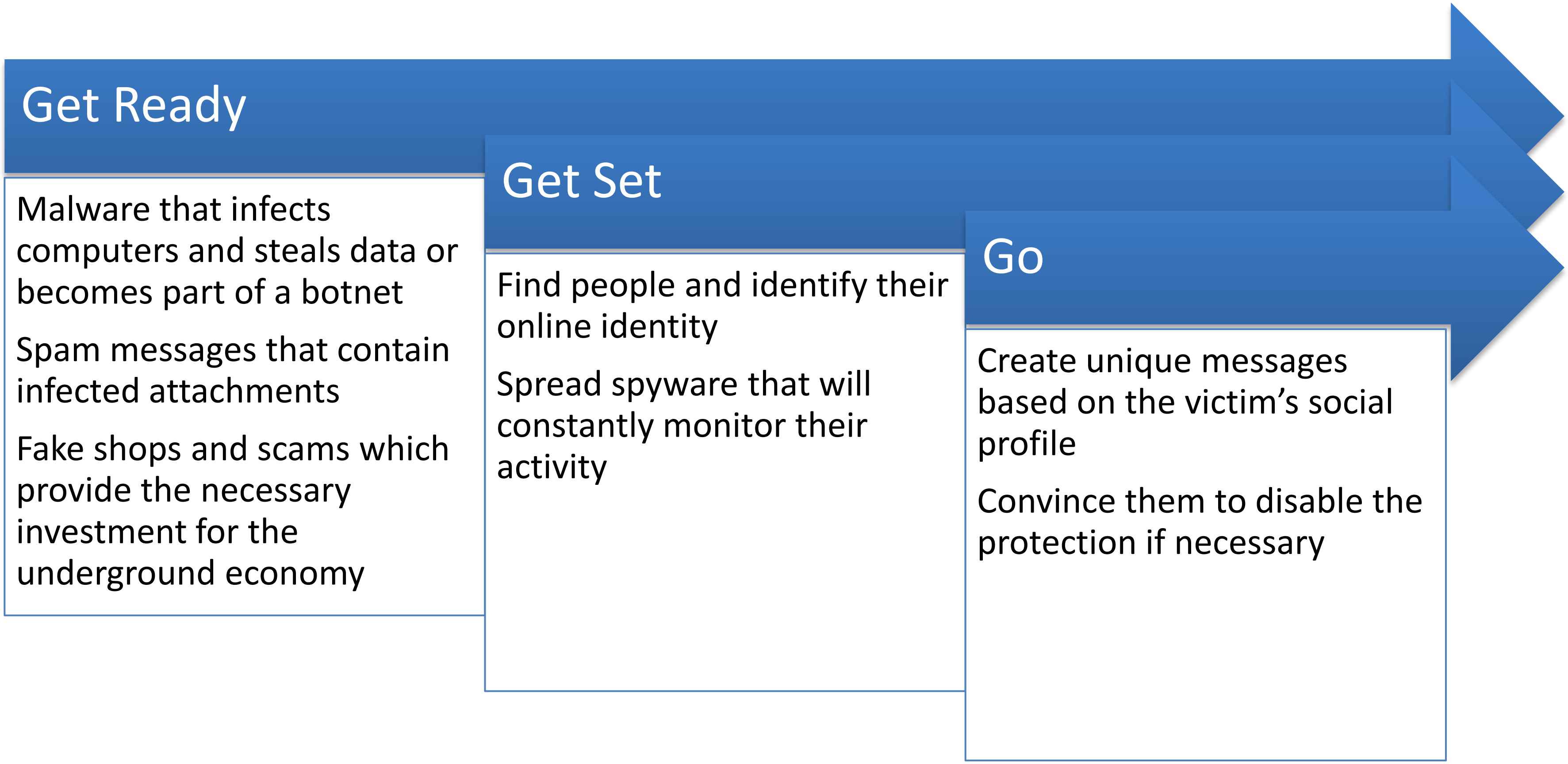
Hide your personal info.

Block data-brokers from exposing data about you to identity thieves, scammers and marketers. Learn how »

Copyright@bitdefender 2011 / www.bitdefender.com

Problem Statement

Bitdefender



Get Ready

Malware that infects computers and steals data or becomes part of a botnet

Spam messages that contain infected attachments

Fake shops and scams which provide the necessary investment for the underground economy

Get Set

Find people and identify their online identity

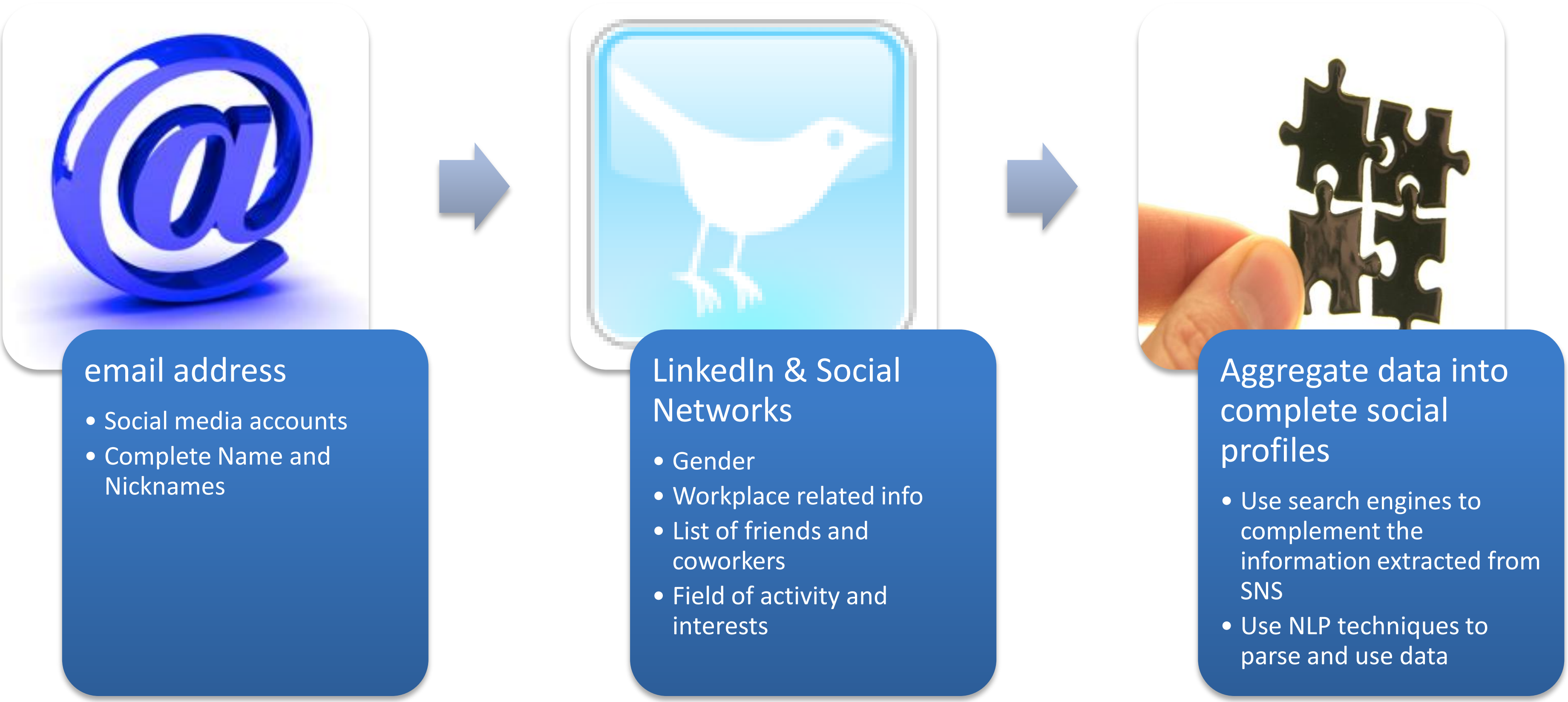
Spread spyware that will constantly monitor their activity

Go

Create unique messages based on the victim’s social profile

Convince them to disable the protection if necessary

Steps of a Targeted Attack



email address

- Social media accounts
- Complete Name and Nicknames

LinkedIn & Social Networks

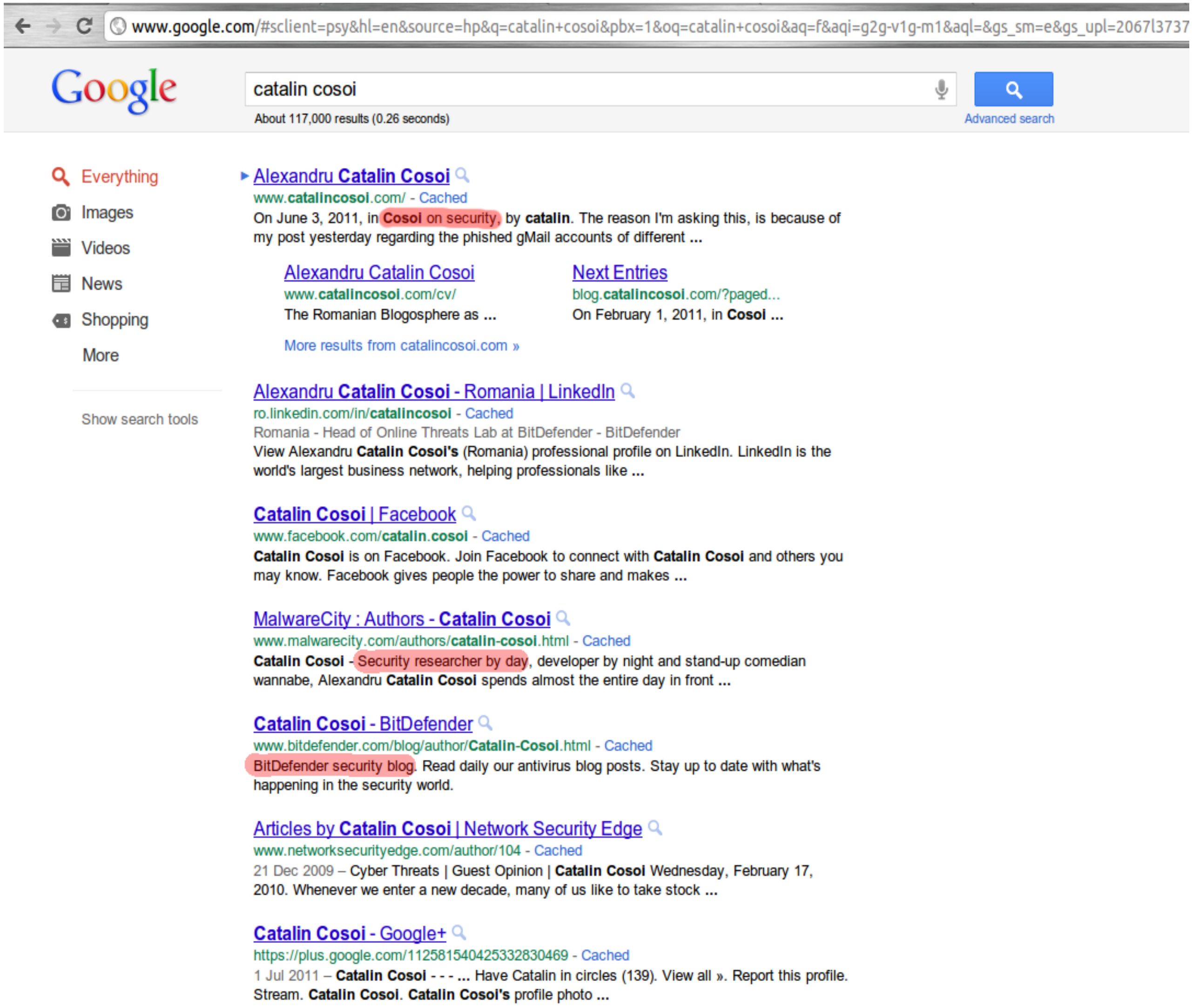
- Gender
- Workplace related info
- List of friends and coworkers
- Field of activity and interests

Aggregate data into complete social profiles

- Use search engines to complement the information extracted from SNS
- Use NLP techniques to parse and use data

Copyright@bitdefender 2011 / www.bitdefender.com

Google search


www.google.com/#sclient=psy&hl=en&source=hp&q=catalin+cosoi&pbx=1&oq=catalin+cosoi&aq=f&aqi=g2g-v1g-m1&aql=&gs_sm=e&gs_upl=2067l3737
Google
catalin cosoi
Advanced search
Everything
Images
Videos
News
Shopping
More
Show search tools

About 117,000 results (0.26 seconds)

[Alexandru **Catalin Cosoi**](www.catalincosoi.com/)
www.**catalincosoi**.com/ - Cached
On June 3, 2011, in **Cosoi** on security, by **catalin**. The reason I'm asking this, is because of my post yesterday regarding the phished gMail accounts of different ...

Alexandru Catalin Cosoi
www.**catalincosoi**.com/cv/
The Romanian Blogosphere as ...

Next Entries
blog.**catalincosoi**.com/?paged...
On February 1, 2011, in **Cosoi** ...

More results from catalincosoi.com »

Alexandru **Catalin Cosoi** - Romania | LinkedIn
ro.linkedin.com/in/**catalincosoi** - Cached
Romania - Head of Online Threats Lab at BitDefender - BitDefender
View Alexandru **Catalin Cosoi's** (Romania) professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like ...

Catalin Cosoi | Facebook
www.facebook.com/**catalin.cosoi** - Cached
Catalin Cosoi is on Facebook. Join Facebook to connect with **Catalin Cosoi** and others you may know. Facebook gives people the power to share and makes ...

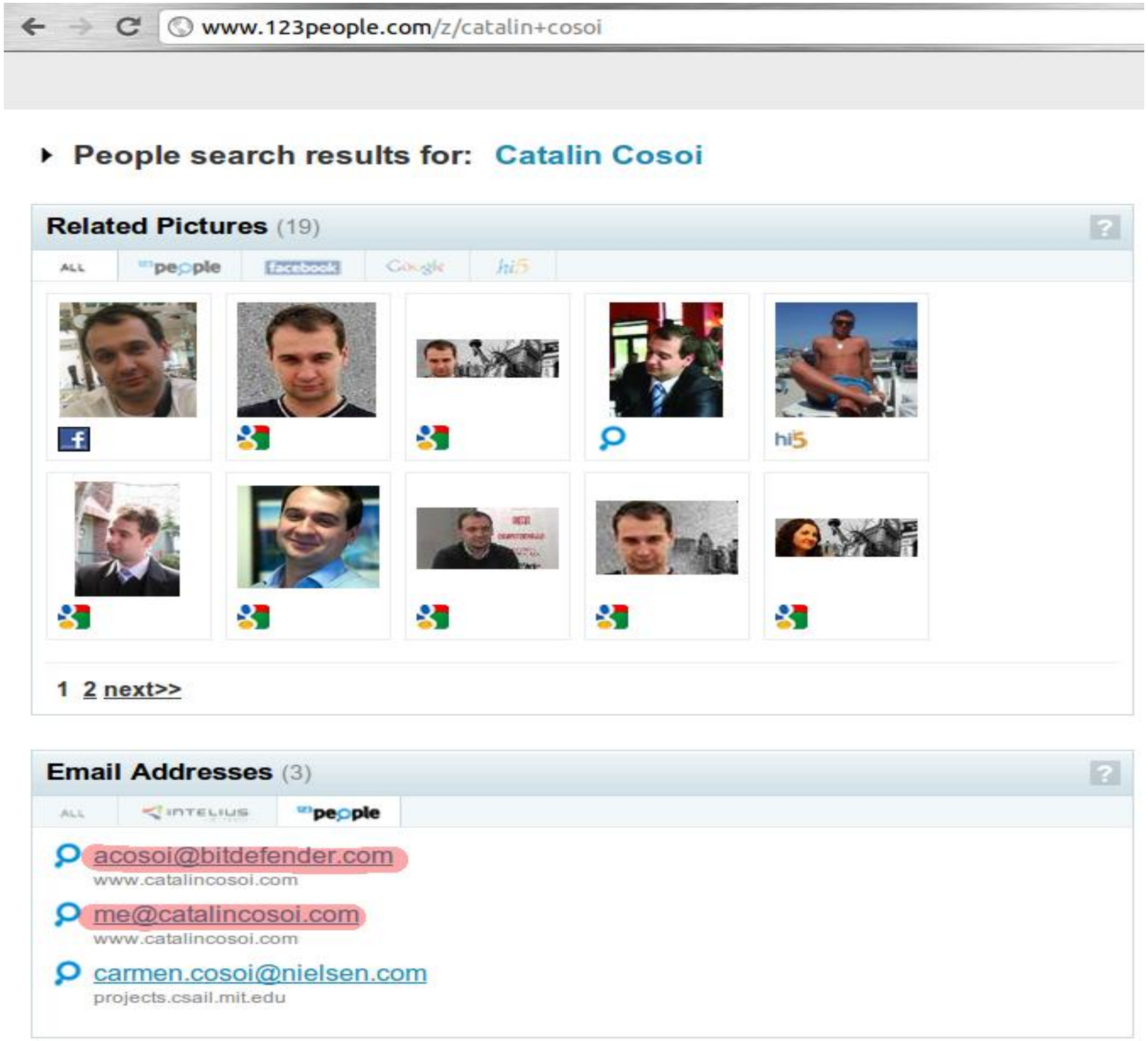
MalwareCity : Authors - **Catalin Cosoi**
www.malwarecity.com/authors/**catalin-cosoi**.html - Cached
Catalin Cosoi - Security researcher by day, developer by night and stand-up comedian wannabe, Alexandru **Catalin Cosoi** spends almost the entire day in front ...

Catalin Cosoi - BitDefender
www.bitdefender.com/blog/author/**Catalin-Cosoi**.html - Cached
BitDefender security blog. Read daily our antivirus blog posts. Stay up to date with what's happening in the security world.

Articles by **Catalin Cosoi** | Network Security Edge
www.networksecurityedge.com/author/104 - Cached
21 Dec 2009 – Cyber Threats | Guest Opinion | **Catalin Cosoi** Wednesday, February 17, 2010. Whenever we enter a new decade, many of us like to take stock ...

Catalin Cosoi - Google+
https://plus.google.com/112581540425332830469 - Cached
1 Jul 2011 – **Catalin Cosoi** - - - ... Have Catalin in circles (139). View all ». Report this profile. Stream. **Catalin Cosoi**. **Catalin Cosoi's** profile photo ...

123people search



www.123people.com/z/catalin+cosoi

People search results for: Catalin Cosoi

Related Pictures (19)

1 2 next>>

Email Addresses (3)

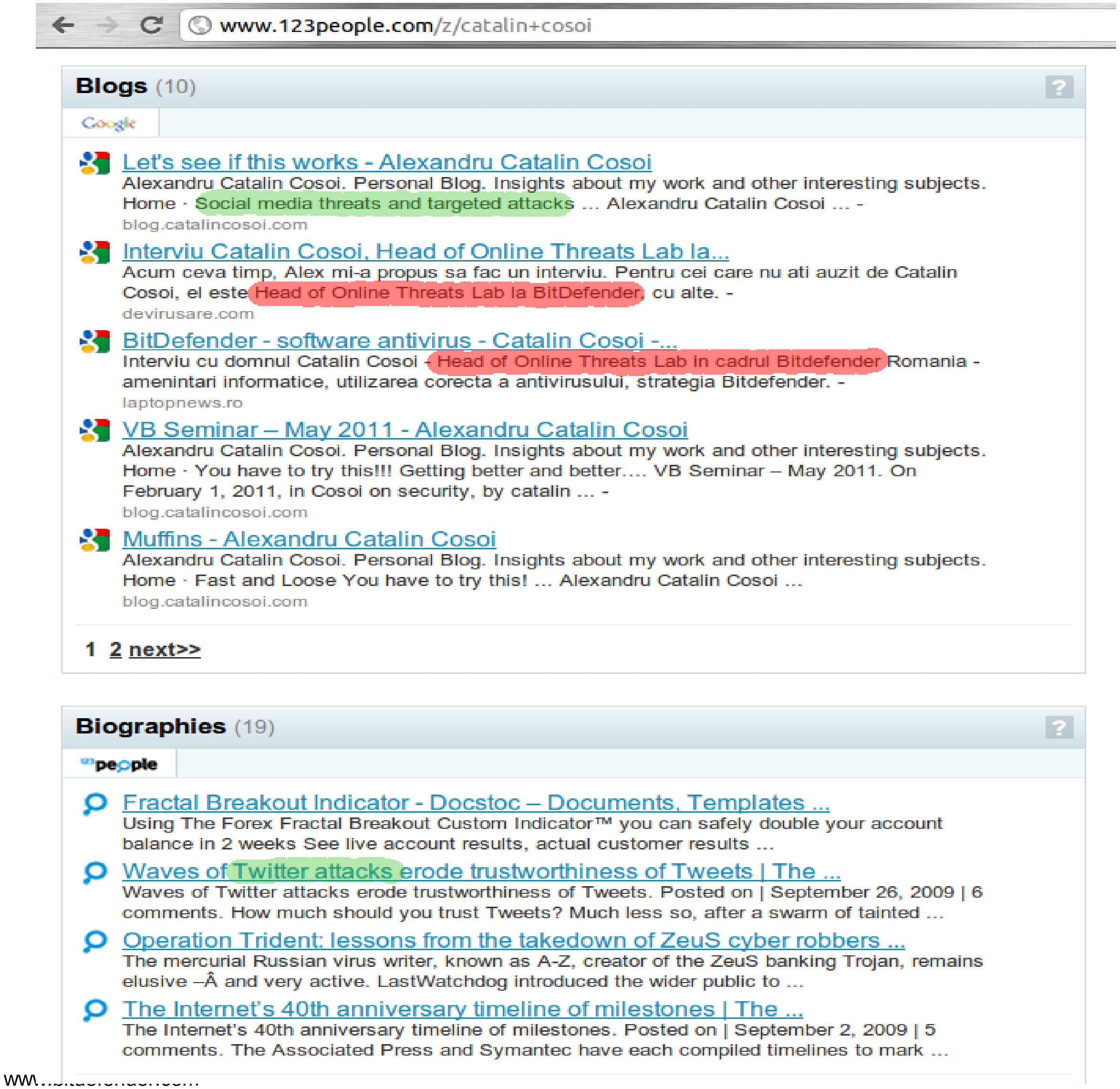
acosoi@bitdefender.com
www.catalincosoi.com

me@catalincosoi.com
www.catalincosoi.com

carmen.cosoi@nielsen.com
projects.csail.mit.edu

123people search

Bitdefender



www.123people.com/z/catalin+cosoi

Blogs (10)

Google

[Let's see if this works - Alexandru Catalin Cosoi](#)
Alexandru Catalin Cosoi. Personal Blog. Insights about my work and other interesting subjects. Home · Social media threats and targeted attacks ... Alexandru Catalin Cosoi ... -
blog.catalincosoi.com

[Interviu Catalin Cosoi, Head of Online Threats Lab la...](#)
Acum ceva timp, Alex mi-a propus sa fac un interviu. Pentru cei care nu ati auzit de Catalin Cosoi, el este Head of Online Threats Lab la BitDefender, cu alte. -
devirusare.com

[BitDefender - software antivirus - Catalin Cosoi -...](#)
Interviu cu domnul Catalin Cosoi - Head of Online Threats Lab in cadrul Bitdefender Romania - amenintari informatice, utilizarea corecta a antivirusului, strategia Bitdefender. -
laptopnews.ro

[VB Seminar – May 2011 - Alexandru Catalin Cosoi](#)
Alexandru Catalin Cosoi. Personal Blog. Insights about my work and other interesting subjects. Home · You have to try this!!! Getting better and better.... VB Seminar – May 2011. On February 1, 2011, in Cosoi on security, by catalin ... -
blog.catalincosoi.com

[Muffins - Alexandru Catalin Cosoi](#)
Alexandru Catalin Cosoi. Personal Blog. Insights about my work and other interesting subjects. Home · Fast and Loose You have to try this! ... Alexandru Catalin Cosoi ...
blog.catalincosoi.com

1 2 next>>

Biographies (19)

people

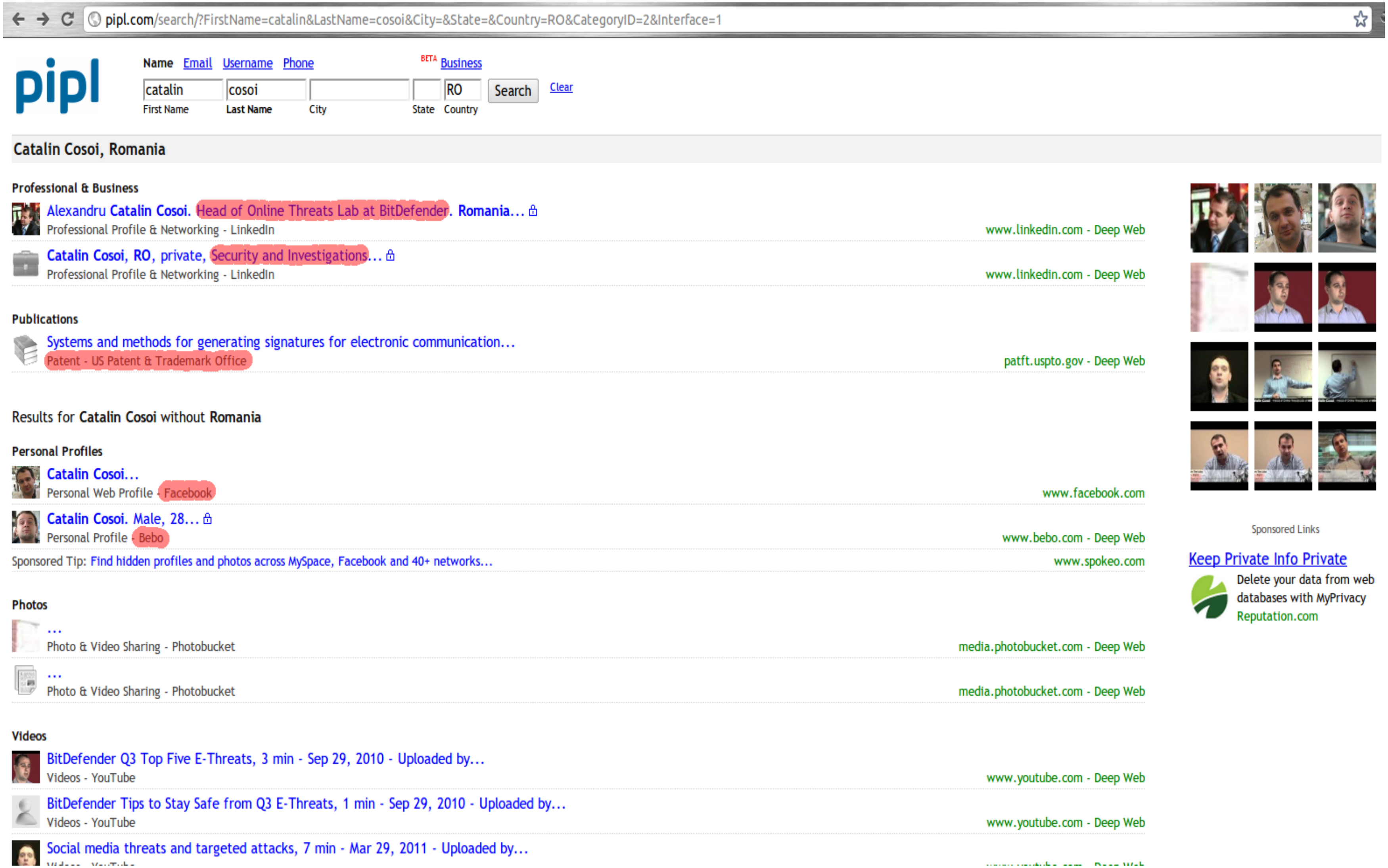
[Fractal Breakout Indicator - Docstoc – Documents, Templates ...](#)
Using The Forex Fractal Breakout Custom Indicator™ you can safely double your account balance in 2 weeks See live account results, actual customer results ...

[Waves of Twitter attacks erode trustworthiness of Tweets | The ...](#)
Waves of Twitter attacks erode trustworthiness of Tweets. Posted on | September 26, 2009 | 6 comments. How much should you trust Tweets? Much less so, after a swarm of tainted ...

[Operation Trident: lessons from the takedown of ZeuS cyber robbers ...](#)
The mercurial Russian virus writer, known as A-Z, creator of the ZeuS banking Trojan, remains elusive –Â and very active. LastWatchdog introduced the wider public to ...

[The Internet's 40th anniversary timeline of milestones | The ...](#)
The Internet's 40th anniversary timeline of milestones. Posted on | September 2, 2009 | 5 comments. The Associated Press and Symantec have each compiled timelines to mark ...

Pipl search



pipl.com/search/?FirstName=catalin&LastName=cosoi&City=&State=&Country=RO&CategoryID=2&Interface=1

First Name: catalin
Last Name: cosoi
City:
State:
Country: RO

Catalin Cosoi, Romania

Professional & Business

Alexandru Catalin Cosoi. Head of Online Threats Lab at BitDefender. Romania...
Professional Profile & Networking - LinkedIn — www.linkedin.com - Deep Web

Catalin Cosoi, RO, private, Security and Investigations...
Professional Profile & Networking - LinkedIn — www.linkedin.com - Deep Web

Publications

Systems and methods for generating signatures for electronic communication...
Patent - US Patent & Trademark Office — patft.uspto.gov - Deep Web

Results for **Catalin Cosoi** without **Romania**

Personal Profiles

Catalin Cosoi...
Personal Web Profile - Facebook — www.facebook.com

Catalin Cosoi. Male, 28...
Personal Profile - Bebo — www.bebo.com - Deep Web

Sponsored Tip: Find hidden profiles and photos across MySpace, Facebook and 40+ networks... — www.spokeo.com

Photos

...
Photo & Video Sharing - Photobucket — media.photobucket.com - Deep Web

...
Photo & Video Sharing - Photobucket — media.photobucket.com - Deep Web

Videos

BitDefender Q3 Top Five E-Threats, 3 min - Sep 29, 2010 - Uploaded by...
Videos - YouTube — www.youtube.com - Deep Web

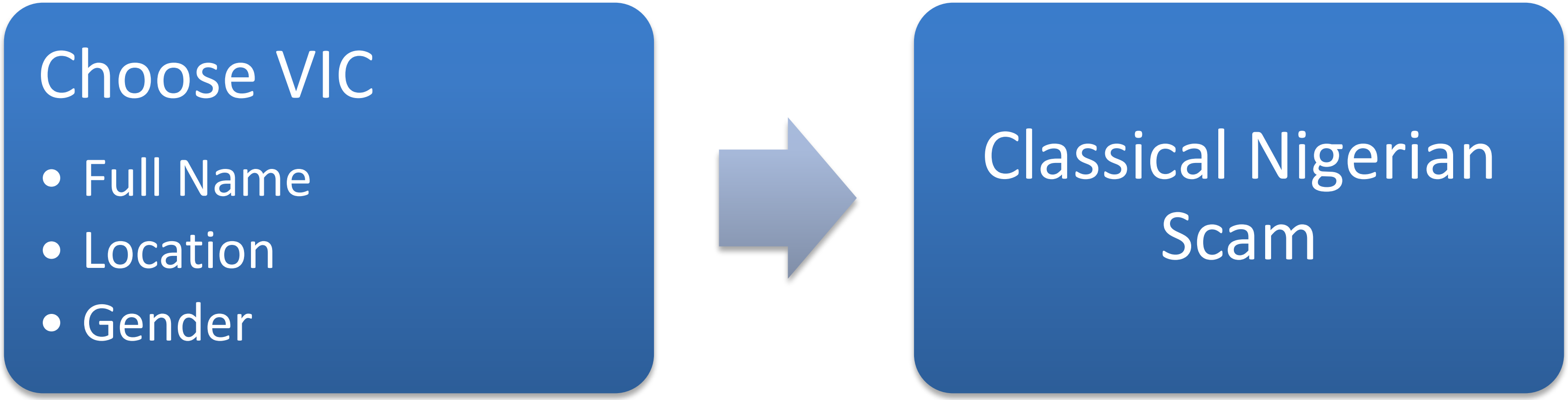
BitDefender Tips to Stay Safe from Q3 E-Threats, 1 min - Sep 29, 2010 - Uploaded by...
Videos - YouTube — www.youtube.com - Deep Web

Social media threats and targeted attacks, 7 min - Mar 29, 2011 - Uploaded by...
Videos - YouTube — www.youtube.com - Deep Web

Sponsored Links

Keep Private Info Private
Delete your data from web databases with MyPrivacy
Reputation.com

Example 1 - background



Choose VIC

- Full Name
- Location
- Gender

Classical Nigerian Scam

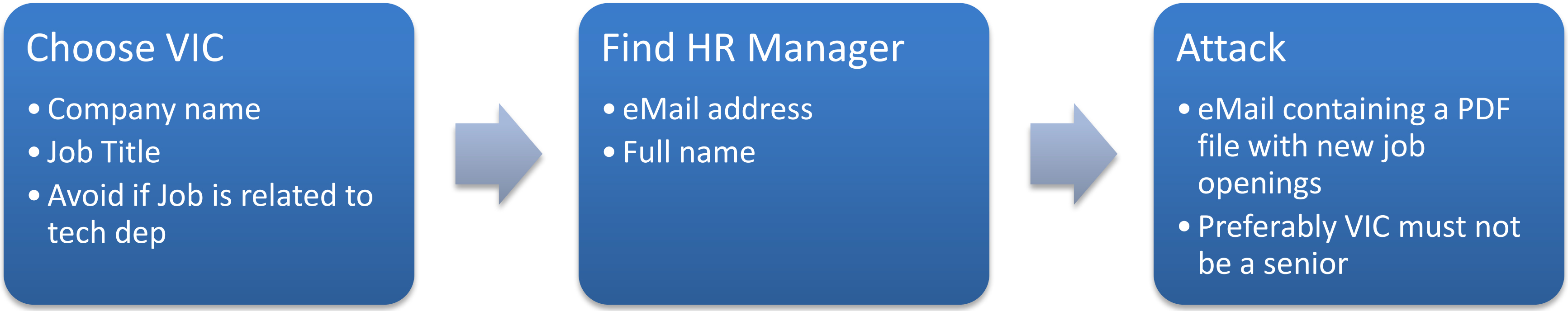
Example 1 - context

Dear Alexandru Cosoi,

I'm writing to you in a time of sadness and desperation. I'm not sure if you know this, but two decades ago, your cousin, *[insert random Romanian name]* Cosoi moved to Nigeria. Here he managed to start a shipment business which in time managed to become quite successful. He has two sons *[another random Romanian name here]* Cosoi and *[yet another random Romanian name here]* Cosoi, which moved to UK. Your cousin is dying, bla bla bla, so we need to transfer money out of Nigeria to UK, in order to provide a decent living for his kids.

We ask for your help because you are family and we wouldn't bother you if it weren't important, and also, it would be better to keep this between us.

Example 2 - background



Choose VIC

- Company name
- Job Title
- Avoid if Job is related to tech dep

Find HR Manager

- eMail address
- Full name

Attack

- eMail containing a PDF file with new job openings
- Preferably VIC must not be a senior

Copyright@bitdefender 2011 / www.bitdefender.com

Example 2 - context

Dear [full name]

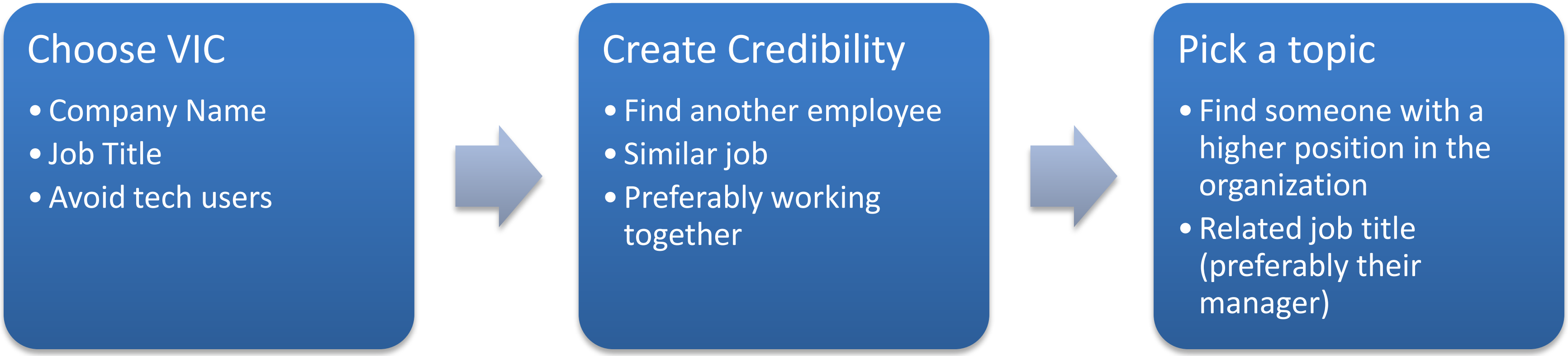
Since we’ve been very pleased with your activity so far, I would like to take this opportunity to thank you for your dedication and involvement.

As the HR team is starting a new project of personal development to boost our employees’ career plans, please find attached the PDF file containing what we believe to be a successful career plan for you in this company.

HR Director

Copyright@bitdefender 2011 / www.bitdefender.com

Example 3 - background



Choose VIC

- Company Name
- Job Title
- Avoid tech users

Create Credibility

- Find another employee
- Similar job
- Preferably working together

Pick a topic

- Find someone with a higher position in the organization
- Related job title (preferably their manager)

Copyright@bitdefender 2011 / www.bitdefender.com

Example 3 - context

Dude!!! (also knowing the gender helps)

Have you seen the news?!

http://www.getInfected.com

Is it just me, or [manager name] is leaving us?

I’m very very upset that we have to find out about this from the media and not directly from him/her.

Grrrr!!!

Copyright@bitdefender 2011 / www.bitdefender.com

Experiment

- 1996 randomly selected email addresses
- 100 registered a LinkedIn account (5%)
- 370 registered a Facebook account (18.5%)
- 70 registered a Pulse account (3.5%)

- Nickname or Real Name found for 540 individuals
- A valid photo was found for 427 individuals (21%)
- Gender was found for 540 users and determined for an additional 178

Copyright@bitdefender 2011 / www.bitdefender.com

Wrapping up

1. Social engineering works.
2. Social engineering can be automated
3. The better your identity is represented online, the higher the chances of becoming a victim
4. We need to understand the addiction to social networks and the fact that users will post information about themselves online, ignoring the consequences.
5. Education can work. It’s our duty to educate both users and employees about social engineering and how their own data can turn against them.

Bitdefender®