Automated targeted attacks

the new age of cybercrime

Ștefan Tănase

Senior Security Researcher
Global Research and Analysis Team

Virus Bulletin 2010 - Vancouver, Canada

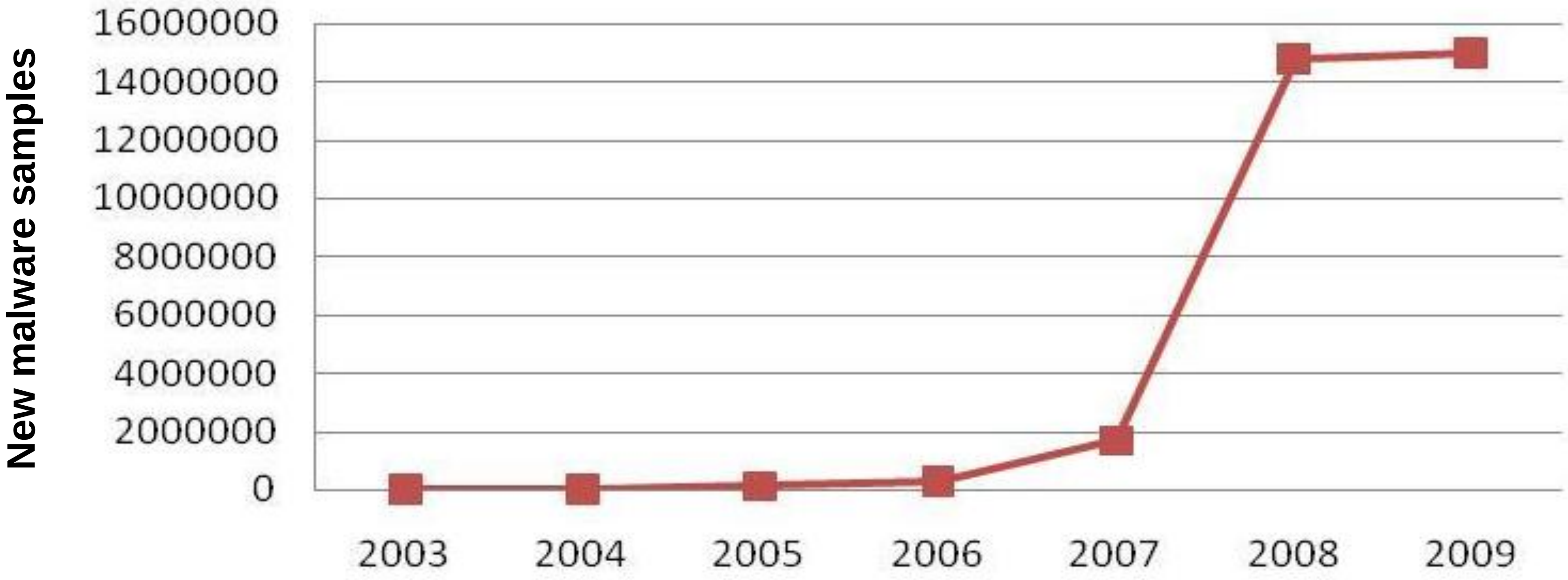
Overview - Targeted Attacks

- The (R)evolution of **malware**
- **Motivation:** how cybercriminals **make money**
- **Targeted attacks:** threats to **SMBs** & **enterprises**
- So, **how do they do it**?
  - **Targeted attacks in 4 steps**
- **Live demo**
- **Targeted attacks** becoming **automated**
- **Surviving** targeted attacks

The (R)evolution of **malware**

The evolution of malware

- 1992 – 2007: about **2M unique malware** programs
- **In 2009 alone**: more than **14M new malicious programs**
- **End of Q1,2010:** a total of about **36,2M** unique malicious files in the Kaspersky Lab collection



Motivation for cybercrime

How do cybercriminals make money

- By **stealing**, of course
  - Stealing **directly from the user**
    - Online **banking** accounts, **credit card** numbers, electronic **money**, blackmailing.
  - *What if **I don't have money**?*
  - Providing **IT resources** to other cybercriminals
    - Creating **botnets**, sending **spam**, **DDoS** attacks, pay-per-click **fraud**, affiliate networks, renting **computing power**, collecting **passwords** etc.
  - Providing access to **targeted SMB and enterprise networks** for interested **3rd parties**

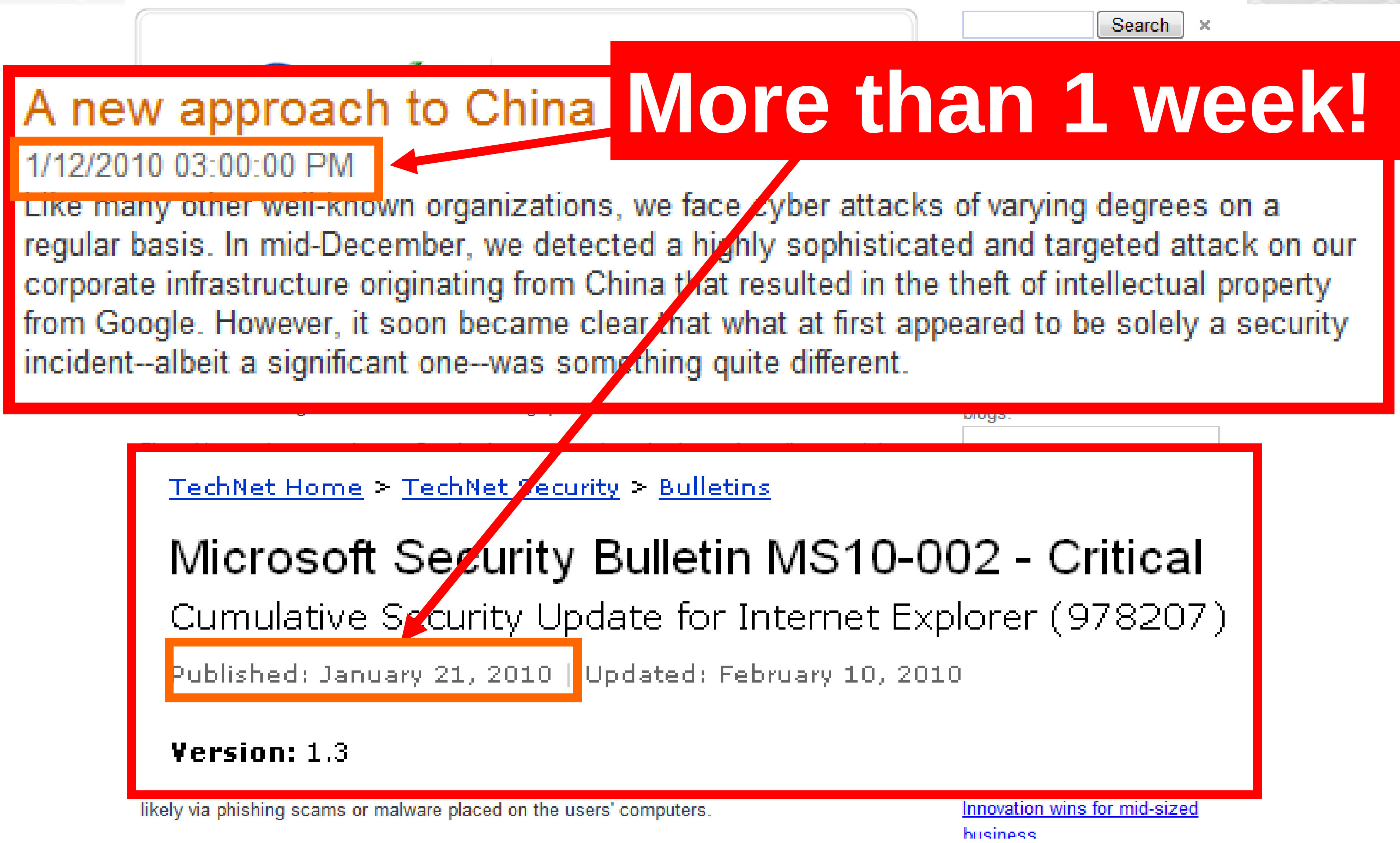
What are they after?

- **What do attackers want?**
  - sensitive **source codes**
  - **future product** information
  - 3rd party **data hosted by the victim**
  - credentials for **production systems**
  - **executive emails**
  - information about **customers**
  - to explore an intranet for **other confidential info**
- **Easily saleable data is not really targeted**

CONFIDENTIAL

Targeted attacks: threats to **SMBs** & **enterprises**

Targeted attacks: threats to SMBs & enterprises



More than 1 week!

A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

TechNet Home > TechNet Security > Bulletins

Microsoft Security Bulletin MS10-002 - Critical

Cumulative Security Update for Internet Explorer (978207)

Published: January 21, 2010 | Updated: February 10, 2010

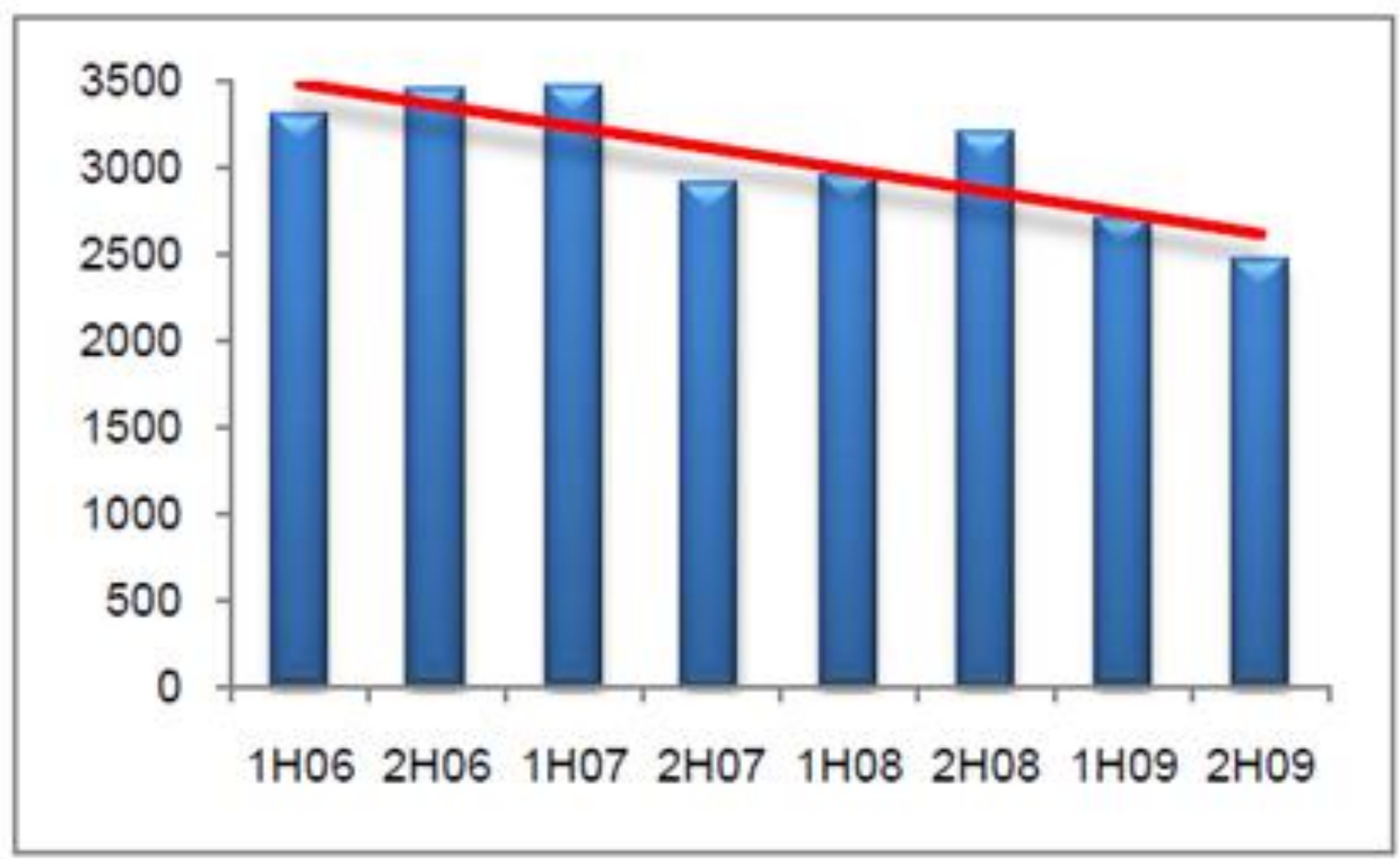
Version: 1.3

likely via phishing scams or malware placed on the users' computers.

Innovation wins for mid-sized business

It only takes a **vulnerability** that has a **window of 1 hour**

Vulnerabilities – There's plenty of them out there



Source: Microsoft Security Intelligence Report Volume 8

Targeted attacks versus classic malware

Lethal injection versus **a hail of bullets**

- **Targeted attacks are not epidemics**
  - One email is enough, instead of tens of thousands
  - Stay under the radar
- **Targeted organizations are either not aware, or don’t publicly disclose information**
  - It is hard to get samples for analysis
- **Classic signature-based AV is useless**
  - Proactive protection technologies
- Much **higher stakes**
  - **Intellectual property theft, corporate espionage**

So, **how are they doing it**?

Targeted attacks in 4 steps

1. **Profiling the employees**
   - Choosing the **most vulnerable targets**
   - **Reconnaissance** via **social networks**, **mailing list posts**, public **presentations**, etc
   - Attackers are more comfortable in their own language
   - Language can offer **clues** to the origins of the attack
   - **They worry about getting the good stuff later**

Targeted attacks in 4 steps

2. **Developing** a new and **unique malware attack**
   - Doesn't have to **bypass all AV solutions**, just the one used by the victim
   - Using **social engineering** to get the victim to **click on a link**
     - Gather **OS, browser, plug-in versions** – useful for vulnerabilities
   - **Corporate monoculture** leads to problems
     - Different employees using the same **same software**

Targeted attacks in 4 steps

3. **Gaining control** and **maintaining access**
   - Initial exploit **drops malware** onto victim machine
   - Networks are usually protected from **outside threats**
   - **C&C communication** is done over **TLS or TLS-like protocols**
     - Encryption proves to be a double edged sword
     - Traffic can't be detected

Targeted attacks in 4 steps

4. Getting the 'good stuff' out

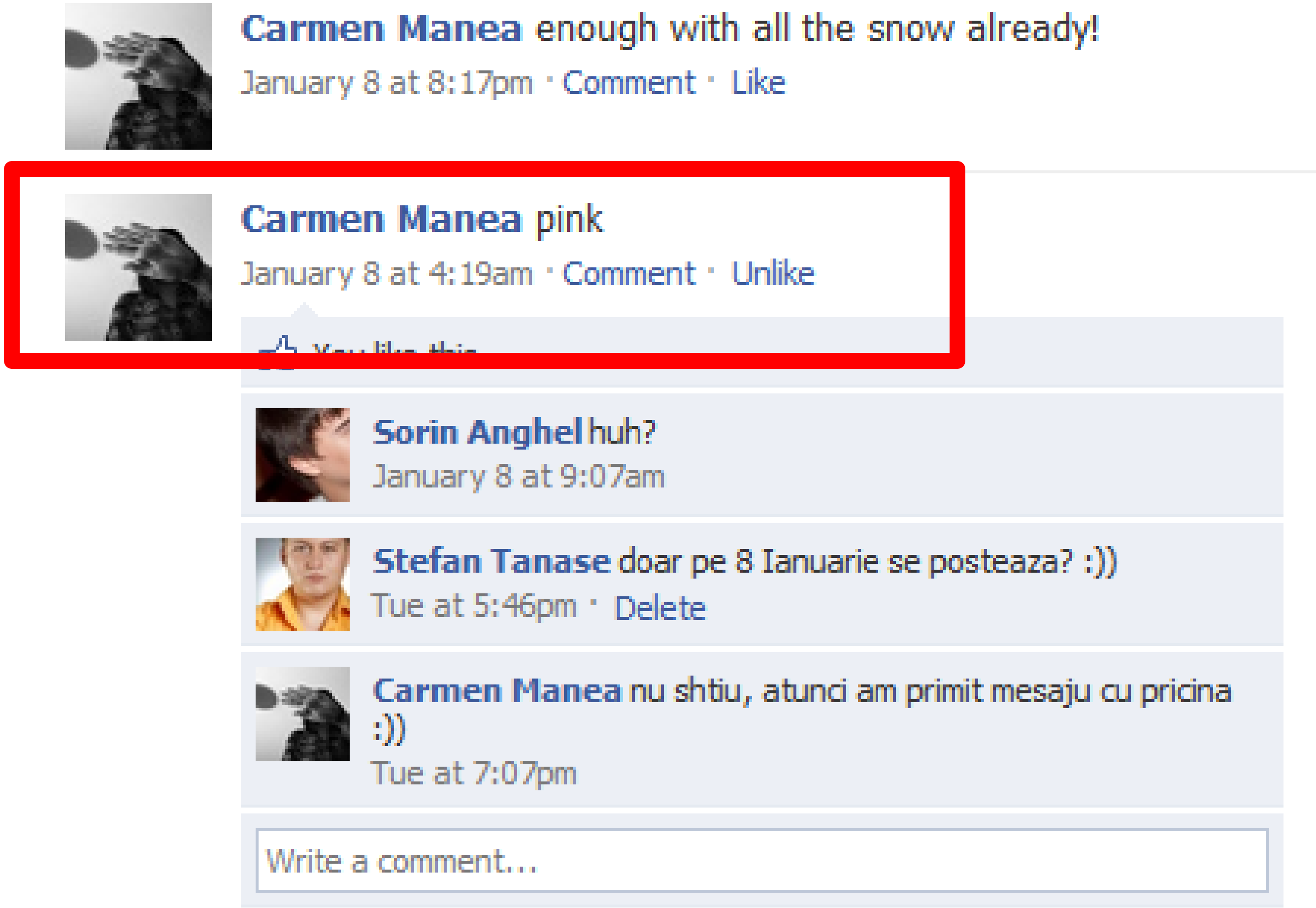
- Find an **overseas office server** to be used as an **internal drop**
  - Speed is the key
- **Move data** over the **corporate WAN/intranet** to the internal drop
- **Get all of the data out at once** to the **external drop server**
  - Even if traffic is monitored, it might be too late to react

A targeted attack demo

Social experiment

Experiment – let's stand up!

- "White", "black", "pink"… "**not wearing any**" ☺



Carmen Manea enough with all the snow already!
January 8 at 8:17pm · Comment · Like

Carmen Manea pink
January 8 at 4:19am · Comment · Unlike

You like this

Sorin Anghel huh?
January 8 at 9:07am

Stefan Tanase doar pe 8 Ianuarie se posteaza? :))
Tue at 5:46pm · Delete

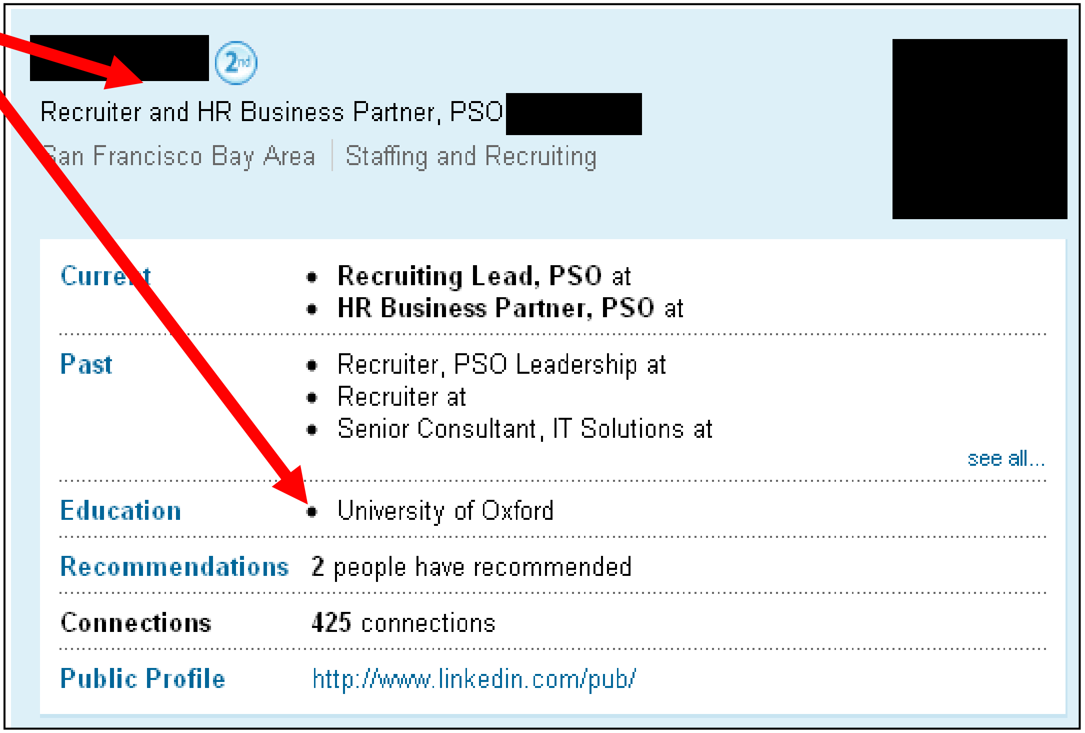
Carmen Manea nu shtiu, atunci am primit mesaju cu pricina :))
Tue at 7:07pm

Write a comment...

Targeted attacks becoming **automated**

Personal information becoming public

- So much **personal information becomes public** on **social networks** right now
- **Advertisers** are already doing it: **targeted ads**
  - Age, gender, location, interests, field of work, browsing habits, relationships etc.



[redacted] 2nd

Recruiter and HR Business Partner, PSO [redacted]

San Francisco Bay Area | Staffing and Recruiting

[redacted]

Current
- **Recruiting Lead, PSO** at
- **HR Business Partner, PSO** at

Past
- Recruiter, PSO Leadership at
- Recruiter at
- Senior Consultant, IT Solutions at

see all...

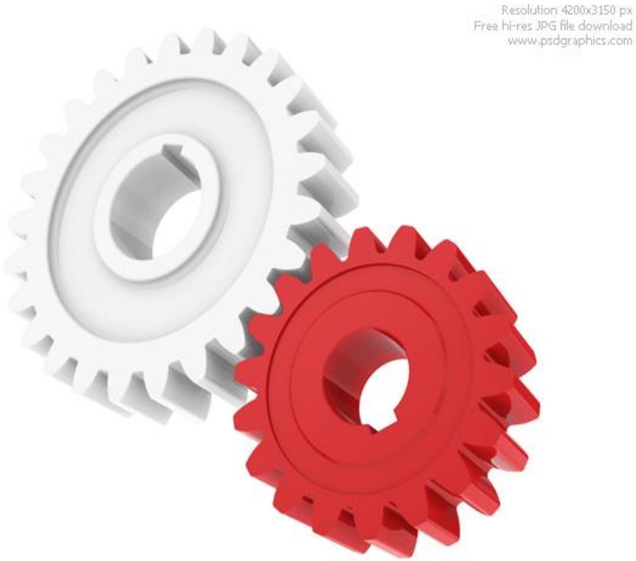
Education
- University of Oxford

Recommendations 2 people have recommended

Connections 425 connections

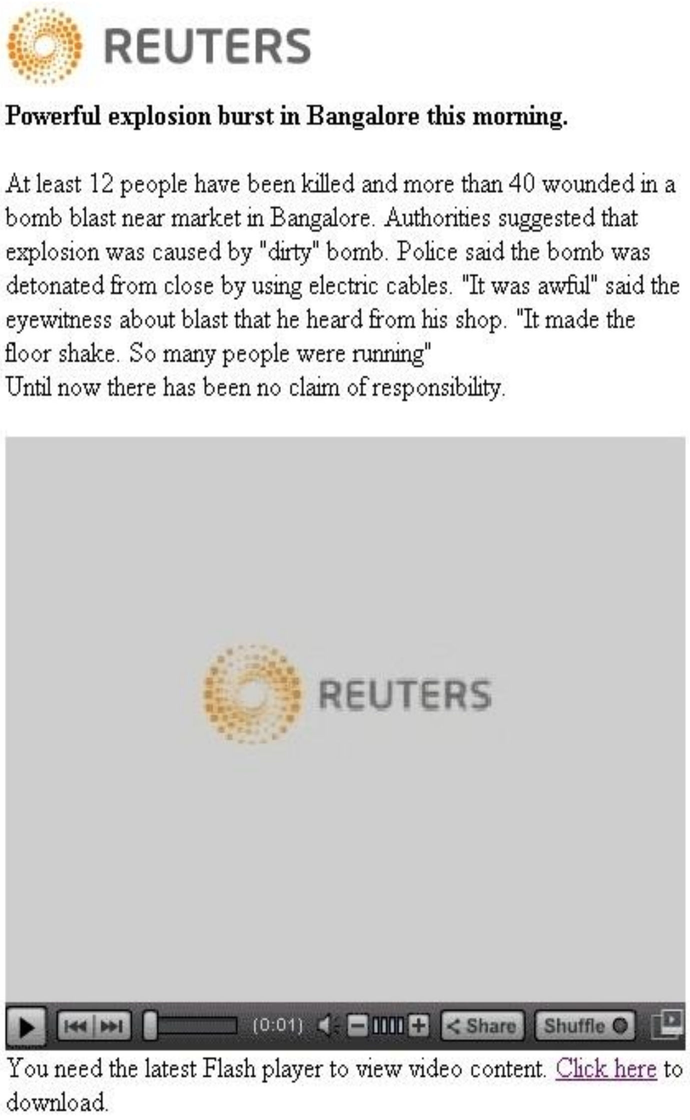
Public Profile http://www.linkedin.com/pub/

Targeted attacks becoming mainstream



- Targeted ads? **Targeted attacks** are already out there
- **Social networks** are enabling cybercriminals to start delivering ***automated targeted attacks***
- **The personal data is there.** Next step? **Automation.**
  - **Geographical IP location** has been around for a while
  - Automatic **language translation services** are becoming better
  - **Personal interests & tastes** are public (ie: **trending topics**)

Geo targeting example



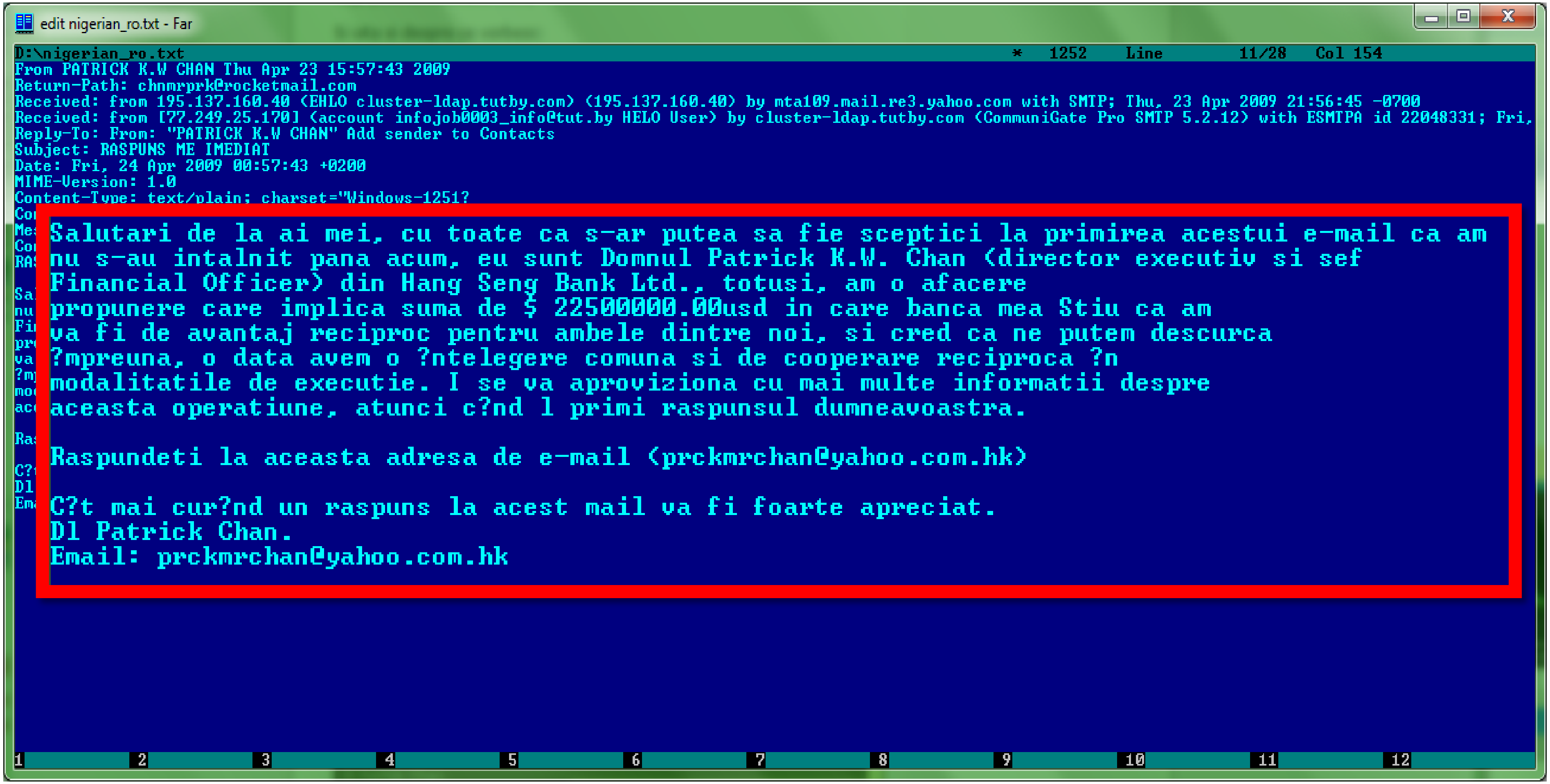
REUTERS

Powerful explosion burst in Bangalore this morning.

At least 12 people have been killed and more than 40 wounded in a bomb blast near market in Bangalore. Authorities suggested that explosion was caused by "dirty" bomb. Police said the bomb was detonated from close by using electric cables. "It was awful" said the eyewitness about blast that he heard from his shop. "It made the floor shake. So many people were running"
Until now there has been no claim of responsibility.

You need the latest Flash player to view video content. Click here to download.

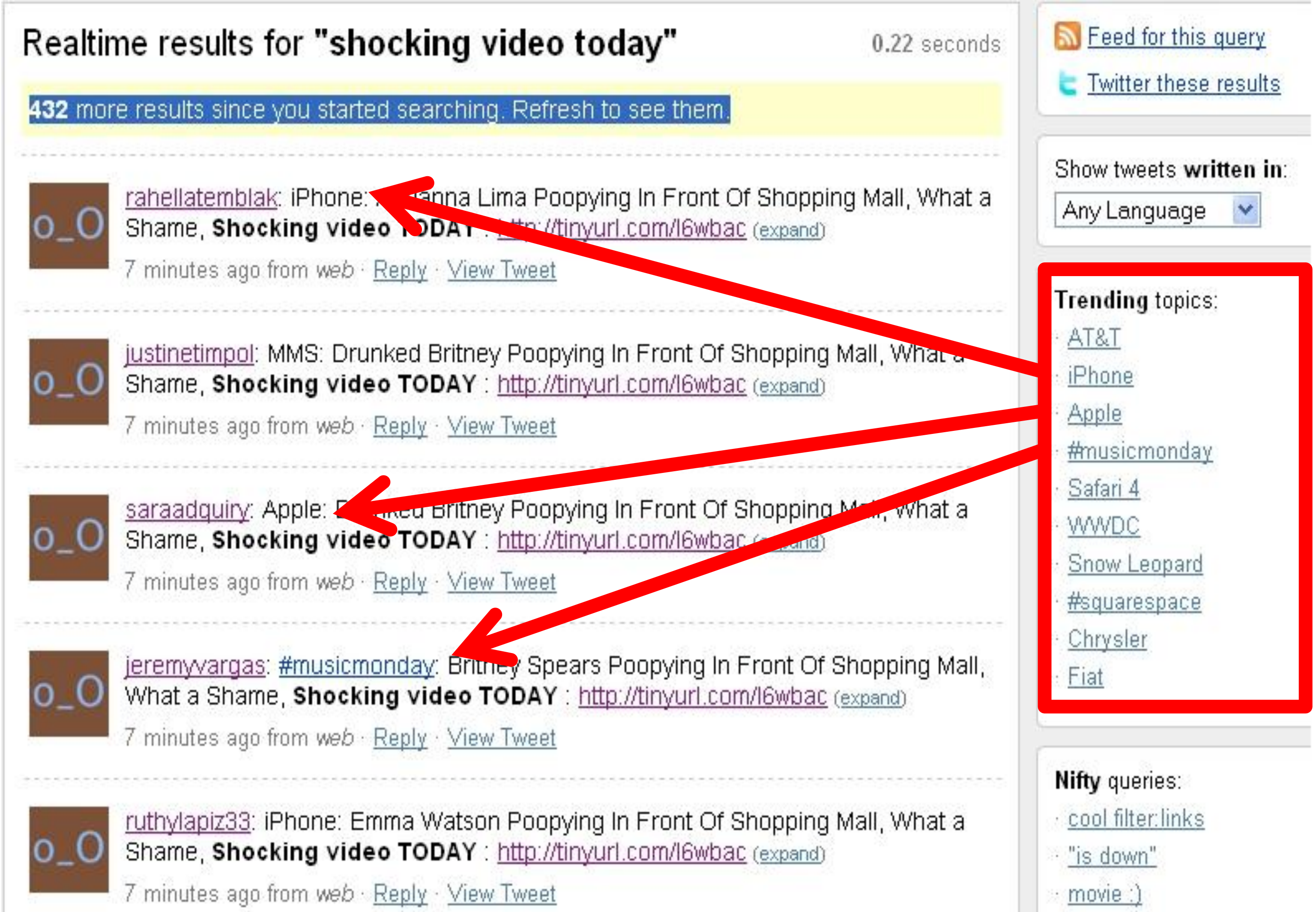
Language targeting example



```
D:\nigerian_ro.txt                                                                                 *  1252    Line        11/28   Col 154
From PATRICK K.W CHAN Thu Apr 23 15:57:43 2009
Return-Path: chnmrprk@rocketmail.com
Received: from 195.137.160.40 (EHLO cluster-ldap.tutby.com) (195.137.160.40) by mta109.mail.re3.yahoo.com with SMTP; Thu, 23 Apr 2009 21:56:45 -0700
Received: from [77.249.25.170] (account infojob0003_info@tut.by HELO User) by cluster-ldap.tutby.com (CommuniGate Pro SMTP 5.2.12) with ESMTPA id 22048331; Fri,
Reply-To: From: "PATRICK K.W CHAN" Add sender to Contacts
Subject: RASPUNS ME IMEDIAT
Date: Fri, 24 Apr 2009 00:57:43 +0200
MIME-Version: 1.0
Content-Type: text/plain; charset="Windows-1251?
Co
Me
Co
RA

Sa
nu
Fi
pr
va
?m
mo
ac

Ra

C?
Dl
Em
```

```
Salutari de la ai mei, cu toate ca s-ar putea sa fie sceptici la primirea acestui e-mail ca am
nu s-au intalnit pana acum, eu sunt Domnul Patrick K.W. Chan (director executiv si sef
Financial Officer) din Hang Seng Bank Ltd., totusi, am o afacere
propunere care implica suma de $ 22500000.00usd in care banca mea Stiu ca am
va fi de avantaj reciproc pentru ambele dintre noi, si cred ca ne putem descurca
?mpreuna, o data avem o ?ntelegere comuna si de cooperare reciproca ?n
modalitatile de executie. I se va aproviziona cu mai multe informatii despre
aceasta operatiune, atunci c?nd l primi raspunsul dumneavoastra.

Raspundeti la aceasta adresa de e-mail (prckmrchan@yahoo.com.hk)

C?t mai cur?nd un raspuns la acest mail va fi foarte apreciat.
Dl Patrick Chan.
Email: prckmrchan@yahoo.com.hk
```

Interests targeting example



Realtime results for "shocking video today" 0.22 seconds

432 more results since you started searching. Refresh to see them.

rahellatemblak: iPhone: Adrianna Lima Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)

7 minutes ago from web · Reply · View Tweet

justinetimpol: MMS: Drunked Britney Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)

7 minutes ago from web · Reply · View Tweet

saraadquiry: Apple: Drunked Britney Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)

7 minutes ago from web · Reply · View Tweet

jeremyvargas: #musicmonday: Britney Spears Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)

7 minutes ago from web · Reply · View Tweet

ruthylapiz33: iPhone: Emma Watson Poopying In Front Of Shopping Mall, What a Shame, **Shocking video TODAY** : http://tinyurl.com/l6wbac (expand)

7 minutes ago from web · Reply · View Tweet

Feed for this query

Twitter these results

Show tweets **written in**: Any Language

Trending topics:

- AT&T
- iPhone
- Apple
- #musicmonday
- Safari 4
- WWDC
- Snow Leopard
- #squarespace
- Chrysler
- Fiat

Nifty queries:

- cool filter:links
- "is down"
- movie :)

Before we end

Before we end

Before we end

A **highly determined** targeted attacker **will eventually succeed**

Surviving targeted attacks

Surviving targeted attacks

- **Proper security mindset**
  - Lack of user **education** and **awareness**
  - **Training** and **policies**
  - Employee **reporting process**
    - Employees should report **attempted attacks**
    - Companies should have a **follow-up process** for such incidents
  - **24/7 security team** with extremely **fast reaction time**

Surviving targeted attacks

- **Minimize the attack surface**
  - **Fewer 3rd party plug-ins**:
    Flash, Acrobat, Java
  - Use **alternative browsers**
  - Frequent **updates and patches**
- **Proactive protection technologies** provide the necessary edge for remaining secure
  - **Sandboxing** and **virtualization** - isolated environments
  - **HIPS** - Host-based Intrusion Prevention System
  - **Behavioral analysis**
  - **In the cloud** services for fast response

Thank you! Questions?

stefant@kaspersky.ro

twitter.com/**stefant**

Ștefan Tănase

Senior Security Researcher
Global Research and Analysis Team

Virus Bulletin 2010 - Vancouver, Canada