WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE.. BACK HERE
CYBER SECURITY

CyberConflicts of CyberWarriors in the CyberSpace of the new CyberEra

let’s cyberparty like it’s 2012!

(bring your own cyberweapons from home)

INTRODUCTION

About Us

- **Claudio “nex” Guarnieri**
  - Security Researcher at **Rapid7**
  - Core member of **Shadowserver Foundation**
  - Core member of **The Honeynet Project**
  - Creator of **Cuckoo Sandbox**
  - **Twitter @botherder**

About Us

- **Quequero**
  - Collects **mushrooms** for a living
  - Grows **bacteria** for fun
  - **Invents** things to make his Bio longer than nex’s
  - Malware analyst
  - **UIC** Founder: quequero.org
  - **Twitter @quequero**

Pre-CyberEra Intelligence

- Train Agents
  - Infiltrate -> gather -> extract
- Intercept a Contact
  - Bribe -> acquire
- Works on the long term
  - Tends to be expensive and dangerous
  - Agents can defect or switch sides

CyberEra Intelligence

- R&D of your own tools
  - Attack -> gather -> extract
- Works on the short/mid term
  - Less expensive than “standard” intelligence
  - Information is not subjective anymore
  - No danger of betrayal
  - Virtually untraceable
  - No real danger involved… **So far** at least.

Targeted Intrusions !=
APT !=
Cyber Warfare

For one big intrusion covered by the news, there is a **background noise of thousands of attacks** that go under the radar every day.

Myth Busting

- There’s a **big confusion** on the whole thing
- Different **modus operandi**, different **goals**, different **actors**
- Everyone always talk about **China attacking US** and **US attacking Middle East**
- There’s **much more than that!**

When we talk about Targeted Intrusions doesn’t necessarily always have to be state-sponsored.

ASIA REGION

Asia Region

CHINA

兵信息化素养
事高科技人才

Dudes, stop playing Warcraft III!
You gotta attack USA!

Bullshits

1. Huge Chinese cyberarmies
2. Superh4x0rs running ubersophisticated attacks
3. Mostly attacking USA

Groups

- **Several small units** of attackers
  - Around 15-20 groups
  - Around 5-6 constantly active and long-running
- In some cases they seem **coordinated**
- They are **not the final consumers** of the stolen data
- Some of them possibly **contracted**

Modus Operandi

- Each group is generally **dedicated to a specific set of targets** or campaigns
- They employ **different techniques**, malwares, exploits and infrastructures
- Goals:
    - Collecting generic data
    - Spying on individuals/organizations
    - Abuse the target's assets (e.g. crafting rogue certificates from CAs)

Collecting Data

- Some groups are **dedicated to collect any data on specific type of organizations or industries**
- They are very **opportunistic**: infect what they can, act quickly and steal what they can
- They don't necessarily go after a specific organization
- They often try to **spread "recursively"** to all the contacts they can harvest from initial victims

Spying on Individuals

- Not much to say, straightforward.
- Generally less opportunistic and more resilient.

Abuse Target’s Assets

- Occurring less often
- **Very well planned** and executed operations
- Eventually quick and dirty as they **hit and run**

Targets

1. **Political dissidents** and **Human-rights activists**
2. **Tibetan** activists and Tibetan organizations
3. **Uyghur** population within China
4. **Taiwanese** government organizations
5. Geographical proximities for territory control
6. Western **governments**, big **energy** and **financial** organizations and **defense contractors**

Techniques

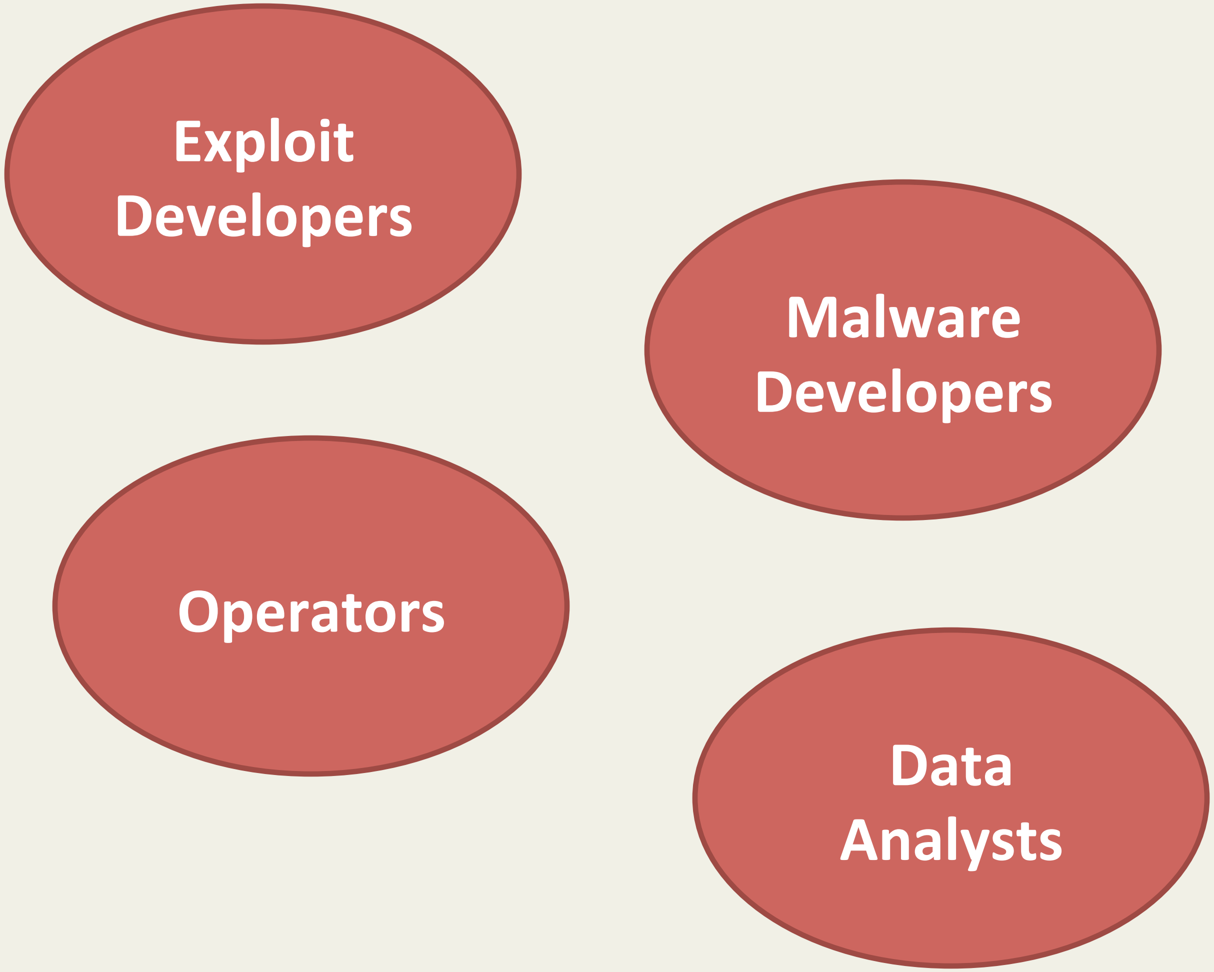
- **Spearphishing**
- Always using **client-side** exploitation
- Sometimes using 0day exploits
  - Microsoft Office
  - Acrobat Reader
  - Flash Player
- Malware artifacts most of the times very simple and **unsophisticated**

Different targets, different tactics

- The amount of attacks against other **Asian** individuals/organizations **is huge**
  - Generally **unsophisticated**
- The amount of attacks against **Western** is **consistent**, but not as huge (although is very difficult to estimate)
  - Generally **more sophisticated**

Division of Labor

- Different sophistication between exploit production and malware production:
  - **Exploits probably acquired by brokers** or independent researchers
  - Or developed by different teams



Exploit Developers

Malware Developers

Operators

Data Analysts

Exploits

- CVE-2010-3333
  - Microsoft Word RTF File Parsing Stack Buffer Overflow Vulnerability
- CVE-2010-2883
  - Stack-based buffer overflow in CoolType.dll in Adobe Reader
- CVE-2011-0611
  - Microsoft Word RTF File Parsing Stack Buffer Overflow Vulnerability
- CVE-2011-2462
  - Vulnerability in the U3D component in Adobe Reader
- **CVE-2012-0158**
  - MSCOMCTL.OCX in the Common Controls in Microsoft Office

Malware

- Each group has its own “flagship malware”
- Most of the times **custom code**
  - Generally basic and unsophisticated for resource **convenience** and **tactical & operational** reasons
- Sometimes also adopting widely known RATs:
  - PoisonIvy
  - Gh0st-RAT

Asia Region

OTHER COUNTRIES

Other Countries

- China is definitely the biggest player, but not the only one:
  - **Pakistan**
  - **India**
  - **Vietnam**
  - **North/South Korea**
  - **Syria**

Other Countries

- The amount of attacks is much lower
- Tend to be more persistent and long running
- Mostly dealing with **political conflicts** within the Asian region
  - e.g.: India vs Pakistan
- They clearly have less resources and therefore adopt known exploits and known trojan kits or acquire commercial solutions

Other Countries

- **Syria**: probably first case of a government acting against their own citizens with cyberattacks
- Targeting rebels with known kits
  - DarkComet
  - Gh0st Rat
- Relying only on **Social Engineering**
- Clearly lacking any type of **know-how**

WESTERN REGION

Europe

- **Benelux** quickly expanding with deep interest in protection of commercial interests and critical infrastructures
- **Denmark** ^
- **Spain** active on the North African frontier
- **UK** & **Germany** active on internal affairs

USA

- Targeted and **sophisticated** attacks
- Tools are developed internally
- 0-days are researched autonomously
- Tech teams are extremely skilled
- For everything else there's… **NSA**

Projects

- **Stuxnet**
  - 0-day exploit***s***, PLC Infection, Signed components
- **Duqu**
  - 0-day exploit, Signed components, Keylogger + Screenshots, Advanced Exfiltration, Modular
- **Flame**
  - **Undisclosed** Cryptanalytic Attack, Signed components, Advanced data extraction capabilities

Stuxnet

- Infected around 130k computers worldwide
- Most of them in Iran
- Highly targeted attack
  - PCS 7, WinCC, Step7
- First worm known to interfere with Industrial Systems
- Used at least in three different variants from 2008 to 2011

Duqu

- Detected infections were less than 50 computers worldwide
  - It used an auto-removal function after 36 days
- Steals Digital Certificates
- Doesn't infect Industrial Systems
- Doesn't propagate
- Used in four different variants from 2008 to 2011
- Written in a language unknown to mankind
  - **OO C compiled in VS 2008 with /O1 /Ob1 :-O**

Flame

- ~360 detected infected machines by Kaspersky's sinkholes
- Records Skype calls, microphone audio, keystrokes, snapshots, network activity
- Steals Text files, **AutoCAD** projects, PDF Documents
- 86 C&C domains registered from 2/Mar/2008 to 16/April/2012
- Possibly the first real-world use of an undisclosed cryptanalytic attack after Enigma

3 Malwares to rule them all

- Stuxnet, Duqu and Flame, to some extent, can all be traced back to 2007/2008
- They serve different purposes: information gathering, intelligence extraction and **sabotage**
- A lot of code is shared among the projects
  - Stuxnet and Duqu share a fair 50%
  - Flame and Stuxnet are highly correlated
- C&C code also appears to be reused

Who came first?

- Order of discovery doesn’t reflect the order of deployment
- Probably they’ve been operating simultaneously
  - *First rule in government spending: why build one when you can have two at twice the price? Only, this one can be kept secret.* (John Hurt talking to Jodie Foster in *Contact*)
- One of those 3 might be the secret child of one single agency

Scenario A

- Let the speculation begin
  - Stuxnet came first
  - Duqu was developed in parallel
- *Stuxnet* released to hit **Natanz** Nuclear Facility
- *Duqu* released almost at the same time to gather further intelligence for next targets
- Stuxnet updated and deployed again
- *Flame* deployed to gather further intelligence

Scenario B

- Duqu deployed and used to gather initial intelligence
- Stuxnet deployed for the first attack
- Flame developed by one single agency to keep surveillance on Iran’s ground
- Stuxnet continued to operate

MIDDLE EAST

Arab World

- Not really active on foreign intelligence activities
- Mostly runs internal politics operations
  - Terrorism
- Technologies imported from foreign countries

Israel

- Vast hi-tech knowledge
- Has some of the world’s best cryptanalysts
  - Adi Shamir, Eli Biham just to name two
- Has one of the world’s best intelligence service
- **Deeply** infiltrated in the Middle East
- Shares a common interest with USA
  - ^{238}U-- -> ^{235}U++ = 0xABAD1DEA
- For everything else there’s… **Unit 8200**

CONCLUSIONS

Future of the CyberWarfare?

- Many countries still have to catch up with the necessary tech skills
- Maghreb, East Africa and Middle East are going to join the party
    - Mostly to manage internal affairs
- Several open questions remain…

Future of the CyberWarfare?

- What is Russia doing now?
  - They are full of talented people, often involved with cybercrimes
- What’s going to be role of Turkey?
- What will happen in South America?
- Are the USA ever going to strike back on China?

The final question

There's something we want to understand:

can CyberWar lead to a **real** old-fashioned war?

Q&A*

* Comic Sans purposely used to make this slide unpleasant