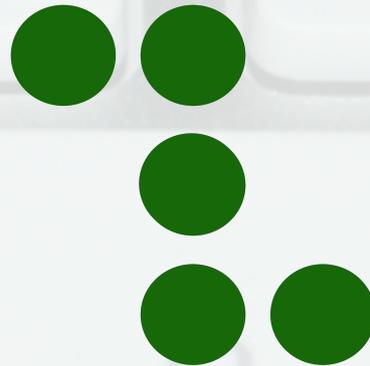


Espionage in Cybertopia

- A Government's Tale -

Sven Herpig
www.zedian.info



Cyber Espionage

Cyber espionage is an attack by any individual, group, organization or state using digital networks, to illegally obtain information with the ultimate outcome to weaken the targeted political unit by potentially obtaining financial value in the process.

=! corporate espionage (w/exceptions)

Cyber Spies

By skill level:

Real Computer Geniuses

Professionals

Opportunists

Script Kiddies

By incentive:

Hacktivist/ Hacker

Cracker/ Criminals

Military/ Intelligence

Terrorists



Virtual Incentives

ADVISE NAMIN SAYO LESTER MARIANO SUNDIN MO TO
"Magtamo ka ng karunungan, magtamo ka ng pagkaunawa." -Kawikaan 4:5



Deep Penetration Agent ng mga Pwet
Get me to Jail if you want!!
Lester Mariano
AMA, BSIT
Cabanatuan City
Certified Fucker
[My Facebook](#)

Money

Fame

Idealism

Fun

Skills

Political Power

Tools

Social Engineering

Cracking

...

...

**Advanced
Persistent Threat
(APT)**



SOCIAL ENGINEERING SPECIALIST
Because there is no patch for
human stupidity

JINX.COM

Connecting the APT Dots

Advanced persistent threats (APTs) are attacks against targeted companies and resources. Typically, a social engineering attack on an employee triggers a series of activities that opens up the company to serious risks.

6 STAGES OF AN APT

Acquire strategic information about the target's IT environment and organizational structure

INTELLIGENCE GATHERING

31% of employers subject employees who post confidential company data on social networking sites to disciplinary action.



Gain entry into a target's network via email, instant messaging, social networking, or software exploitation

POINT OF ENTRY

In an experiment, **87%** of organizations clicked a link related to a social engineering lure.



Ensure continued communication between the compromised host and the C&C server

COMMAND-AND-CONTROL (C&C) COMMUNICATION



Major APT campaigns use web ports to communicate with C&C servers.

Seek valuable hosts that house sensitive information within the target's network

LATERAL MOVEMENT

The techniques used include passing the hash, which elevates an attacker's privileges to that of an administrator, allowing him to gain access to key targets like mail servers.



Identify valuable data to isolate for future data exfiltration

ASSET/DATA DISCOVERY

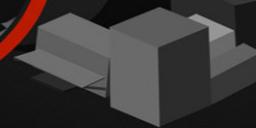
Company secrets comprise **2/3** of enterprises' information portfolios though only half of their security budgets are devoted to protecting these.



Transmit data to a location that the threat actors control

DATA EXFILTRATION

RSA spent **US\$66M** to undo the damage brought about by data exfiltration from its network.



APT MYTHS

Only APTs cause data breaches.



Data breaches result from different types of attacks against an organization. Some data breaches are caused by negligence or malicious insiders.

APTs are isolated incidents.



APTs are considered campaigns and not isolated smash-and-grab incidents. APTs use multiple methods and repeated attempts so the attackers can achieve their goals.

APTs are crafted to extract predetermined files or information.



While attackers may know what kind of information they want to steal, they still require stealth and lateral movement to exfiltrate the specific files they need.

Money is the only motivation behind APT campaigns.



Financial gain is not the attackers' only priority. APT campaigns are conducted against organizations more for cyber espionage or sabotage.

Standard security solutions automatically work against APTs.



There is no silver bullet against APT campaigns but employing specialized detection strategies to monitor your network can greatly reduce risks.

Insight: More sensitive information plus more widespread collaboration increases exposure risks.

Sources:
Detecting the Enemy Inside the Network: How Tough Is It to Deal with APTs?
(http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_apr-primer.pdf)
<http://www.dlapiper.com>
<http://www.social-engineer.org>
<http://egov.aletsonline.com>
<http://www.trendmicro.com>
<http://www.microsoft.com>
<http://about-threats.trendmicro.com>

Damage

Threatlevel

Low to High

Frequency

Daily, Always

Outcome

Economic, Reputation, Health, Power

UNKNOWN Damage

Some 'Incidents'



Titan Rain (2003)

Shady Rat (2006)

GhostNet (2009)

AURORA (2010)

Night Dragon (2011)

**Stuxnet, Duqu, Skywiper
(all 2010-2012)**

Mahdi (2011-2012)

Gauss (2011-2012)

Finfisher (2011-2012)

Shamoon (2012)

'Ghostnet' (2009 - today)

Why 'Ghostnet'

Thorough research and analysis has been conducted inter alia by the Information Warfare Monitor Team and the 'Dark Visitor'.

Clear political intentions and very proper attribution.

Still ongoing: The 'Shadow' Network which is one among three networks still operating after the Ghostnet Shutdown (2010)

'Ghostnet' (2009 - today)

What 'Ghostnet'

- 1300 computers, several countries, Tibetan connections
- Theft of classified and sensitive documents
- Evidence of collateral compromise
- Command-and-control infrastructure that leverages cloud-based social media services
- Links to Chinese hacking community
- Traced to ChengDu, China (e.g. through sinkholes)

'Ghostnet' (2009 - today)

'Ghostnet' Implications:

- Massive loss of data and information
- Disclosed Tibet's Grand Strategy
- Disclosed relations between several countries and Tibet
- Caused international outcry against China
- No severe impact on China even with proper attribution
- Obviously still unpatched systems

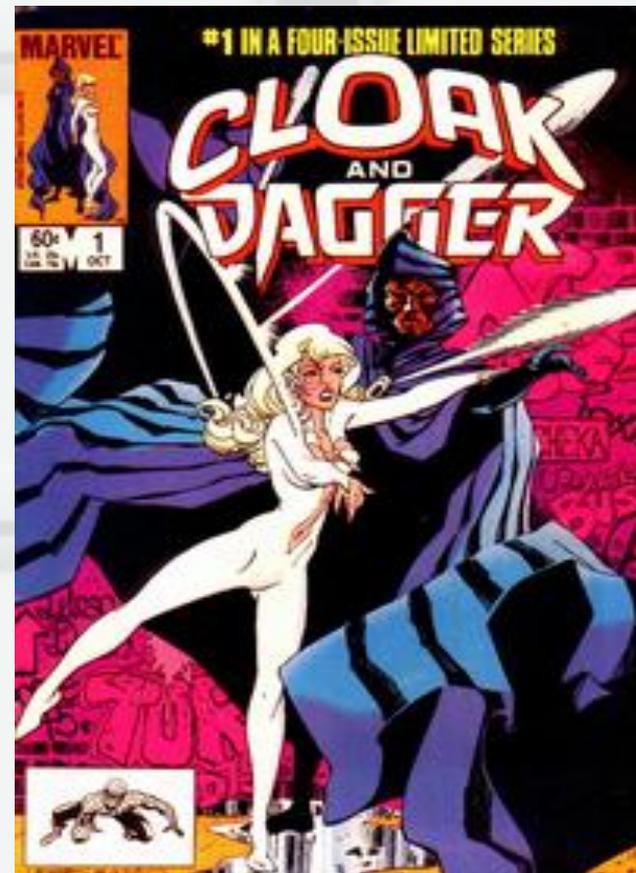
Protecting from Cyber Espionage

Points of Entry:

- 0day exploits
- unpatched exploits
- Wetware

Protection:

- Going Dark + Patches
- Information Security
- Training / Education



<Random Quotes>

"Gauss," as Kaspersky Lab researchers have dubbed the malware, was devised by the same "factory" or "factories" responsible for the Stuxnet worm used to disrupt Iran's nuclear program, as well as the Flame and Duqu Trojans.

Now we have a possible cold war between those states like Iran who are now coding their own malware to attack our systems and to sabotage things to make our lives harder. Is that a war?

Advanced Persistent Threat (APT) has become a tough security challenge that large organizations and important individuals must be prepared for worst sooner or later.

<Random Quotes>

Unlike the largest cybercrime networks that can contain millions of infected computers in a single botnet, cyber-espionage encompasses tens of thousands of infected computers spread across hundreds of botnets,”

Turns out cyberespionage malware and activity is far more prolific than imagined: A renowned researcher has discovered some 200 different families of custom malware used to spy and steal intellectual property

Even more worrisome are the emerging hacking communities in Brazil and the Middle East getting into the act as well. "There's a very active hacking community in the Middle East -- Turkey -- and in Brazil, just like you're seeing with China,"

<Academic Sources>

Clarke, Richard A. and Knake, Robert K. (2010), Cyber War. The Next Threat To National Security And What To Do About It, (New York: Harper-Collings Publisher), pp. 58-62

Nugent, John H. and Raisinghani, Mahesh (2008), 'Bits and Bytes vs. Bullets and Bombs: A New Form of Warfare', in: Janczewski, Lech J. and Colarik, Andrew M. (2008), 'Cyber Warfare and Cyber Terrorism', Information Science Reference, (Hershey and New York: IGI Global), pp. 26-34

FORWARD Consortium (2010), White book: Emerging ICT threats, Deliverable D3.1, FORWARD Consortium, Seventh Framework Programme, Information & Communication Technologies Secure, dependable and trusted Infrastructures, Coordination Action, Grant Agreement no. 216331, pp. 88-92

Fritz, Jason (2008), 'How China will use Cyber Warfare To Leapfrog In Military Competitiveness', Cuoture Mandala, 8, 1, October 2008, pp. 55-56

Gervais, Michael (2011), 'Cyber Attacks and the Laws of War', Yale Law School, <http://ssrn.com/abstract=1939615>, p. 9

Information Warfare Monitor and Shadowserver Foundation (2010), Shadows in the Cloud: Investigating Cyber Espionage 2.0, Joint Report of the Information Warfare Monitor and the Shadowserver Foundation, JR03-2010

Winkler, Ira (2005), 'Guard against Titan Rain hackers', Computer World, 20 October 2005, https://www.computerworld.com/s/article/105585/Guard_against_Titan_Rain_hackers?taxonomyId=017

<News Sources>

<http://arstechnica.com/security/2012/08/nation-sponsored-malware-has-mystery-warhead/>

<http://www.infosecisland.com/blogview/22169-Malware-Wars-Cyber-Wars-Cyber-Espionage-Wars-Oh-My.html>

<http://blog.xecure-isb.com/2012/07/prepare-for-advanced-persistent-threat.html>

<http://krebsonsecurity.com/2012/07/tagging-and-tracking-espionage-botnets/>

<http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240004827/scope-of-aps-more-widespread-than-thought.html>

<http://bits.blogs.nytimes.com/2012/08/13/elusive-finspy-spyware-pops-up-in-10-countries/?smid=tw-share>

<Pictures>

http://www.collider.com/wp-content/uploads/spy_kids_movie_poster_01.jpg

<http://www.set.gov.ph>

http://www.jinx.com/content/prod/143p_0c_1b.jpg

<https://www.intellectuالتakeout.org/sites/www.intellectuالتakeout.org/files/Threat%20Level%20by%20Country.gif>

https://upload.wikimedia.org/wikipedia/en/2/27/Cloak_and_Dagger_1_%281983%29.jpg

<http://www.theprojectxblog.net/book-published-life-and-war-in-cyberspace/>

<https://blog.trendmicro.com/connecting-the-apt-dots-infographic>

<http://phuturenews.com/wp-content/uploads/2011/12/cyber-war.jpg>