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)

@z_edian #theprojectxblog #strategy #ict #development #infosec
Cyber Spies

By skill level:
- Real Computer Geniuses
- Professionals
- Opportunists
- Script Kiddies

By incentive:
- Hacktivist/ Hacker
- Cracker/ Criminals
- Military/ Intelligence
- Terrorists
Virtual Incentives

Money
Fame
Idealism
Fun
Skills
Political Power

ADVISE NAMIN SAYO LESTER MARIANO SUNDIN MO TO
"Magtamo ka ng karumungan, 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 Hacker
My Facebook

@z_edian #theprojectxblog #strategy #ict #development #infosec
Tools

Social Engineering

Cracking

Advanced Persistent Threat (APT)

SOCIAL ENGINEERING SPECIALIST
Because there is no patch for human stupidity
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

INTELLIGENCE GATHERING

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

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

POINT OF ENTRY

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

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

COMMAND-AND-CONTROL (C&C) COMMUNICATION

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

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.

Seek valuable hosts that house sensitive information within the target’s 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.

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

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.

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.

Seek valuable hosts that house sensitive information within the target’s 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.

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

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.

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.

Seek valuable hosts that house sensitive information within the target’s 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.

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

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.

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.

Seek valuable hosts that house sensitive information within the target’s 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.

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

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.

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.

Seek valuable hosts that house sensitive information within the target’s network.
Damage

**Threat level**
Low to High

**Frequency**
Daily, Always

**Outcome**
Economic, Reputation, Health, Power

UNKNOWN Damage
Some 'Incidents' 

- 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)

@z_edian #theprojectxblog #strategy #ict #development #infosec
'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

@z_edian #theprojectxblog #strategy #ict #development #infosec
Protecting from Cyber Espionage

Points of Entry:

- 0day exploits
- unpatched exploits
- Wetware

Protection:

- Going Dark + Patches
- Information Security
- Training / Education
"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 became a tough security challenge that large organizations and important individuals must be prepared for worst sooner or later.
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,"


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


@z_edian #theprojectxblog #strategy #ict #development #infosec
http://www.set.gov.ph
http://www.jinx.com/content/prod/143p_0c_1b.jpg
https://upload.wikimedia.org/wikipedia/en/2/27/Cloak_and_Dagger_1_%281983%29.jpg
https://blog.trendmicro.com/connecting-the-apt-dots-infographic

@z Edian #theprojectxblog #strategy #ict #development #infosec