

Dissecting Advanced Targeted Attacks - Separating Myths from Facts



Candid Wüest
Symantec Corporation

Session ID: SPO-301

Session Classification: General Interest

RSACONFERENCE
EUROPE 2012

How much is Hype or FUD?



NEWS

Hackers Target Japanese Weapons Maker, Nuclear Power Plants

By Matt Peckham on September 20, 2011

CBCnews | Technology & Science

Home World Canada Politics Business Health Arts & Ent

Technology & Science Quirks & Quarks Blog Photo Galleries

Is Canada ready for cyberwar?

CBC News Posted: Mar 13, 2012 1:59 PM ET | Last Updated: Mar 13, 2012 1:58 PM ET 19

Flame: Massive Cyber Superweapon Can Take 'Any Information It Wants' Says Symantec

The sudden discovery of the massive, malicious and highly targeted cyber weapon 'Flame' is like "nothing we've ever seen", security firm Symantec has told the Huffington Post.



Home UK World Companies Markets Global Economy Lex Comment
Business Economy UK Companies Politics & Policy UK Small Companies London 2012 Olympics

September 4, 2012 8:25 pm

Ministers warn on threat from cyber attacks

By Brian Groom, Business and Employment Editor

Cabinet ministers will warn FTSE 100 bosses on Wednesday that responsibility must start at board level if they are to counter the growing threat to their operations from cyber attacks.



Common malware flood

**5.5 Billion
attacks
blocked in 2011**



**1.7 Million
new malware
variants / day**

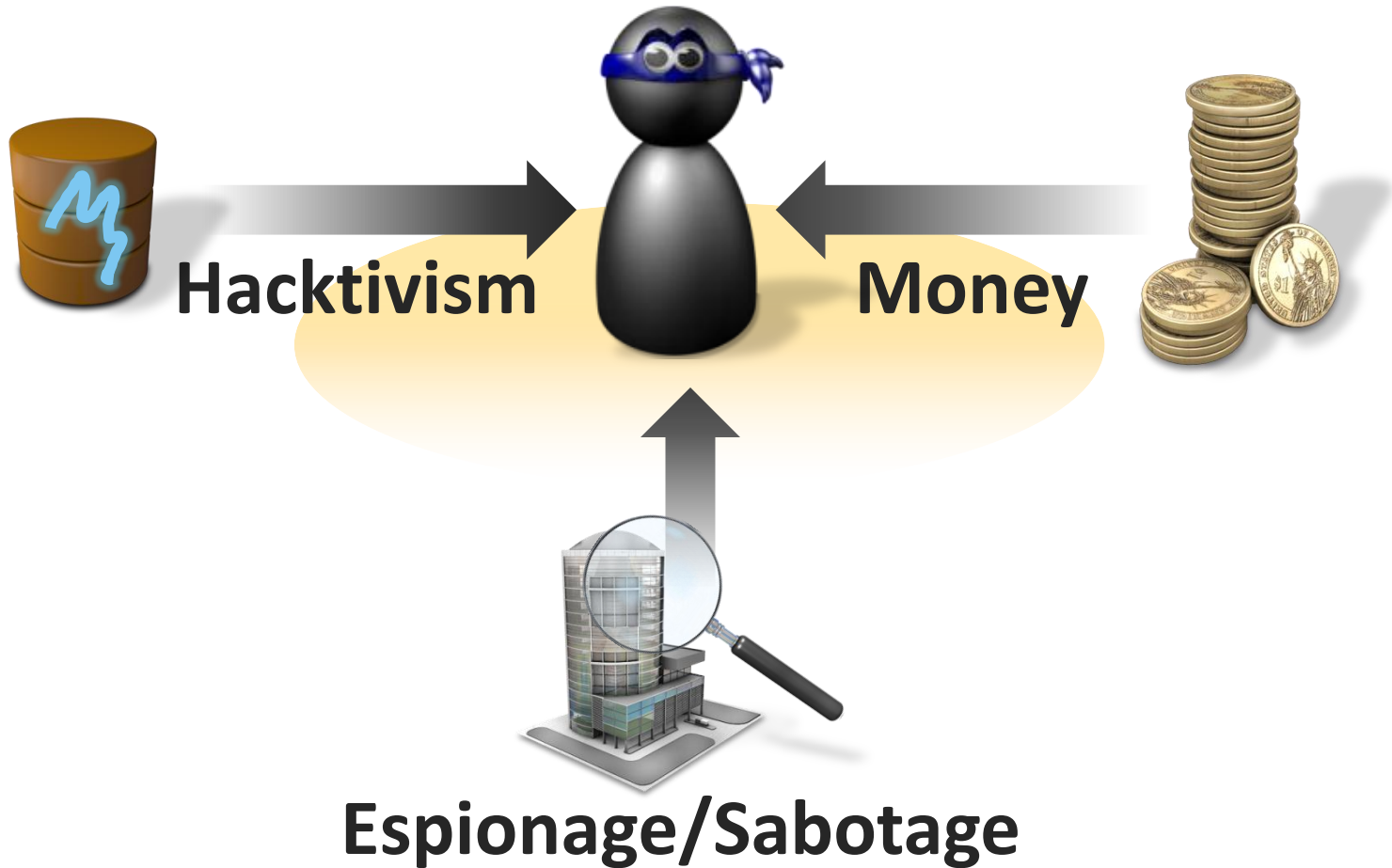


Targeted attacks come on top

151 targeted attacks
identified per day

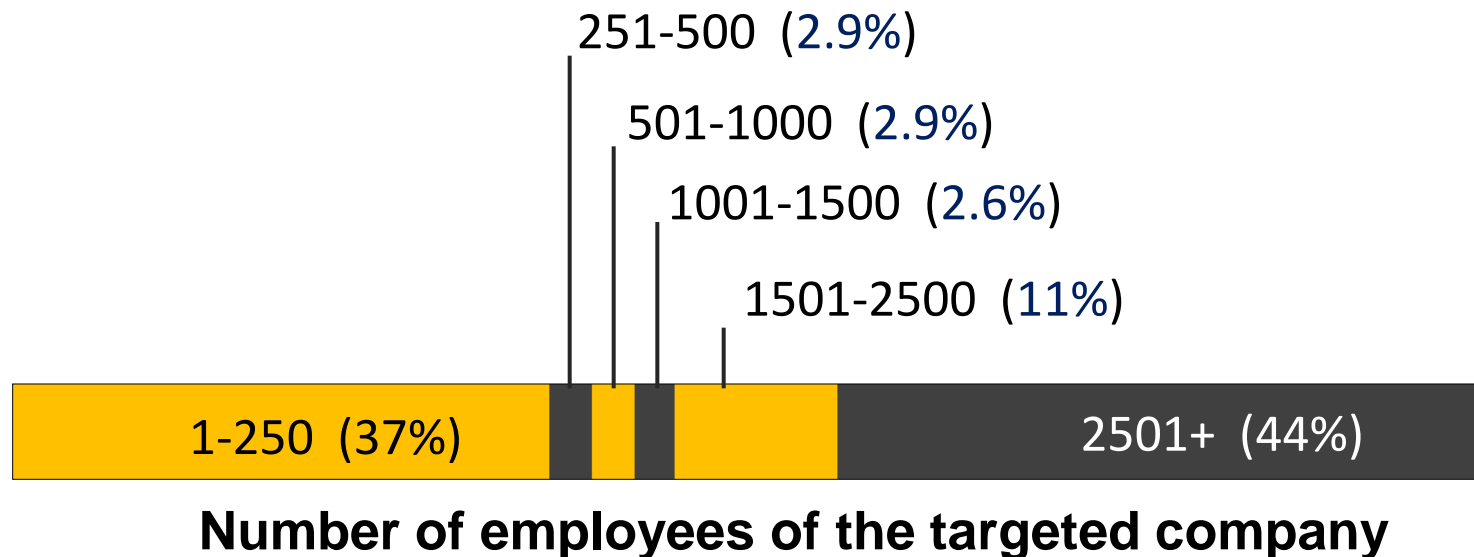


Different motives - Different attacks

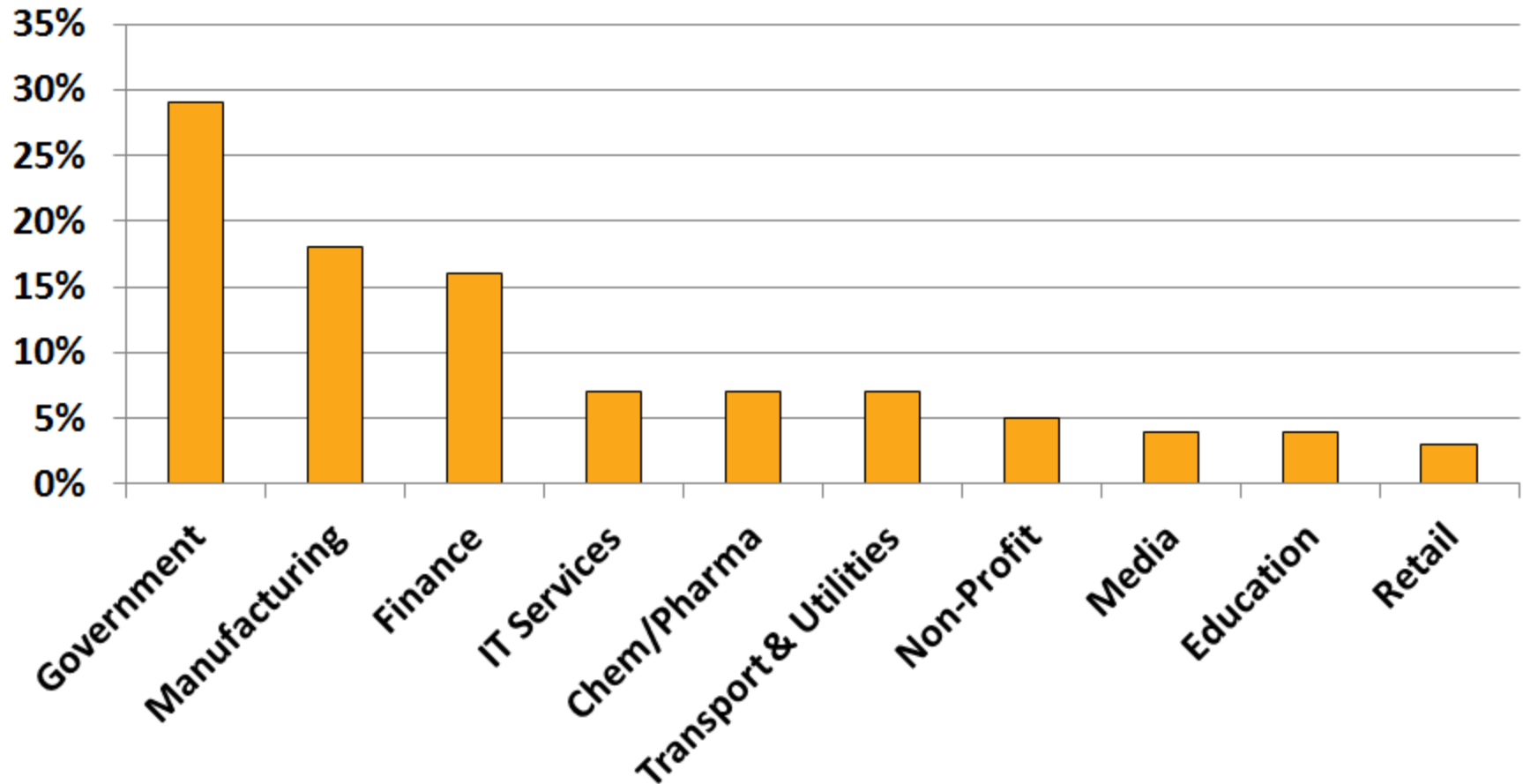


Size does (not) matter

- Small businesses are often not well protected
- but connected to others, used as stepping stones



Targeted attacks by sector



Source: Symantec ISTR 17



Phases of targeted attacks

Reconnaissance

Incursion

Discovery

Capture

Exfiltration



Reconnaissance



Reconnaissance

Find data on possible targets for attack preparation

- Social networks are a gold mine
 - Befriend someone, learn what they want
 - Well-meaning employee post & click a lot

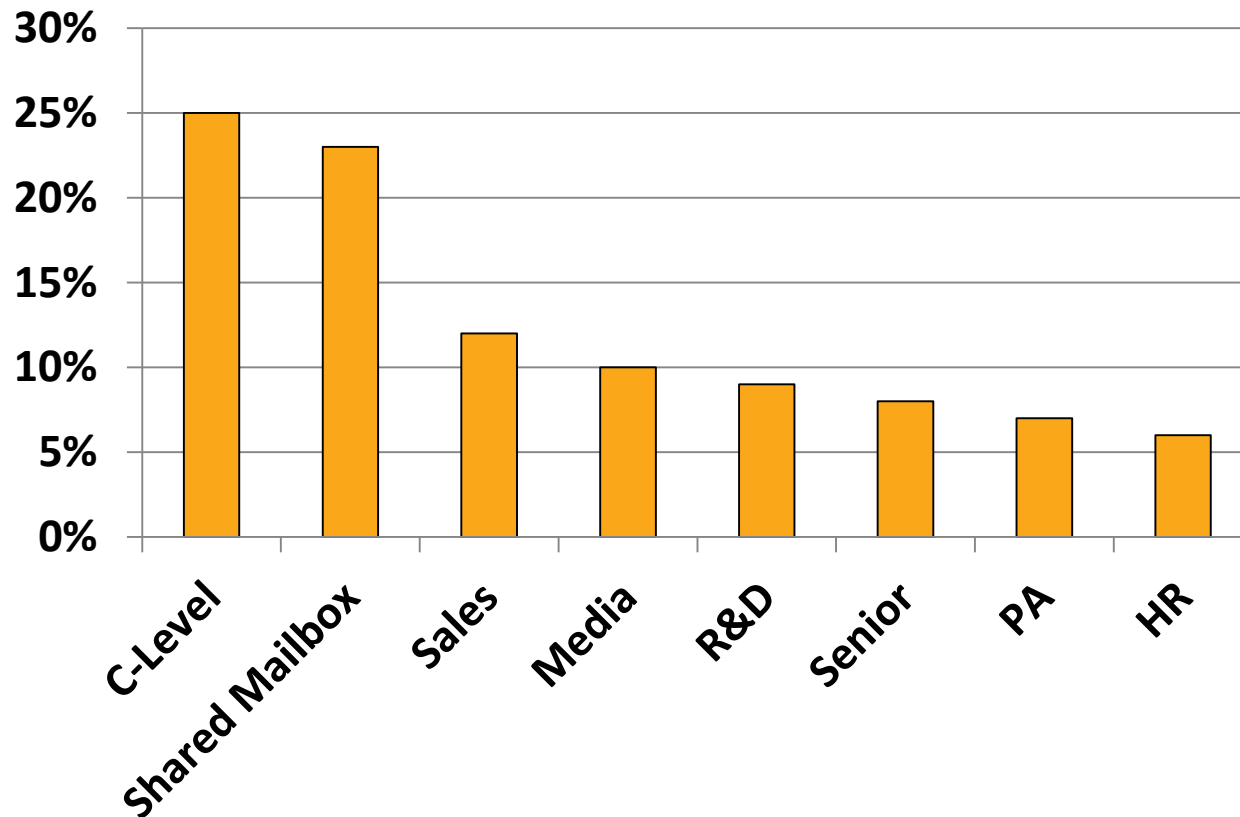
The attackers know the key people and know which protection you have deployed

Protection: User awareness, social media policy



Targeted attacks by targeted person

- Not only CEOs are targeted



Source: Symantec ISTR 17



Incursion



Incursion

The actual „hack“ or break in

- Often combination of social engineering and (zero-day) vulnerability
- Use framework for automation
- Smaller campaigns over a long time period



Protection: Intelligence, SIM, critical system protection, AntiSpam, AV,...



The two most common methods

■ Spear Phishing

- Send a few emails to persons of interest
- Add malicious attachment or link to exploit

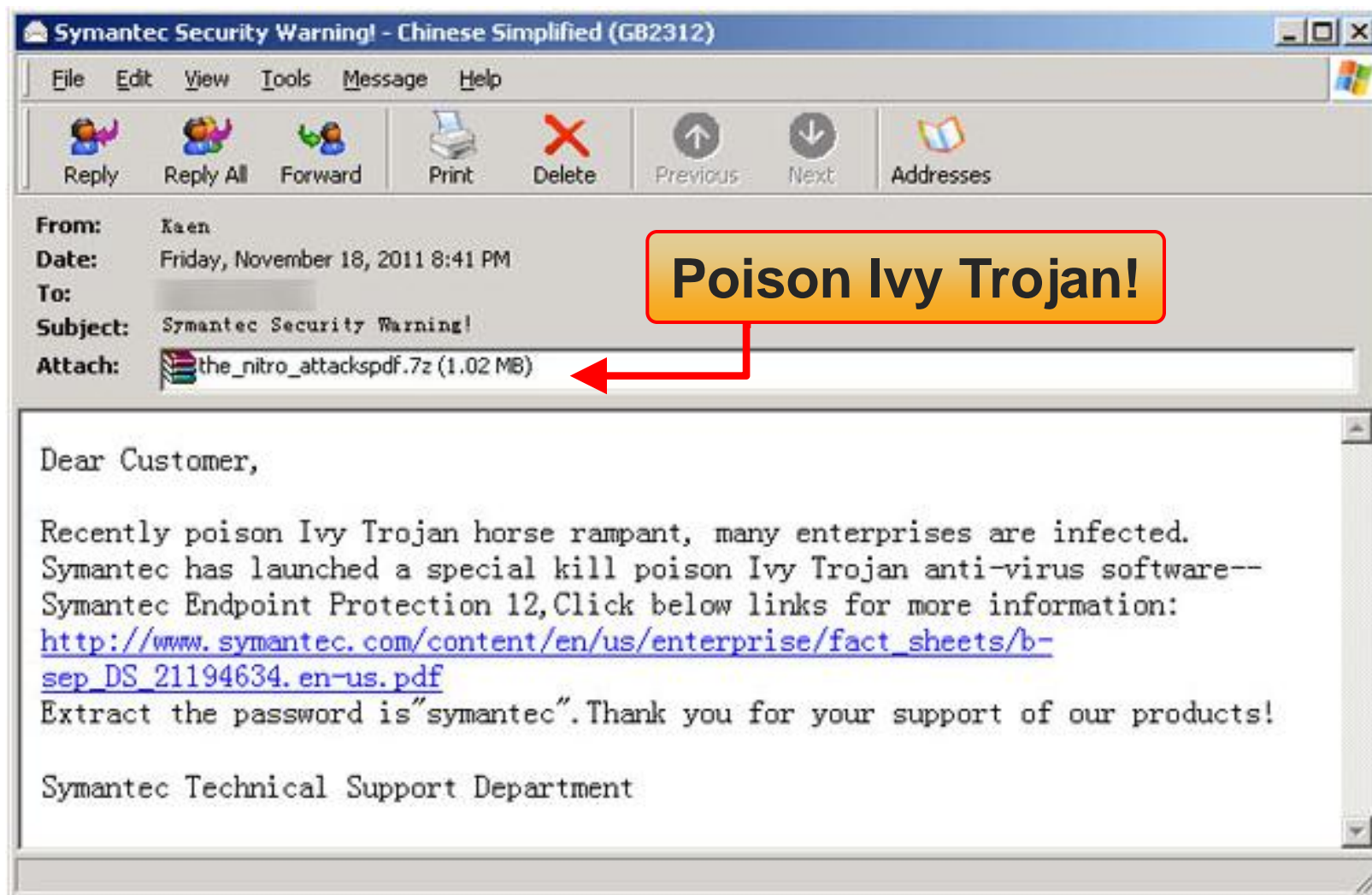


■ Watering Hole Attacks

- Infect a Website of interest to the target user base
- Wait for them to get infected and filter others out



Nitro gang has a sense of humor



Incursion: Examples

Method used:	Elderwood	Taidoor	Stuxnet	Nitro	Duqu	Lucky Cat
Emails with exploit document	0-day	✓		0-day	0-day	✓
Website with exploit	0-day			(0-day)		
USB stick			0-day			



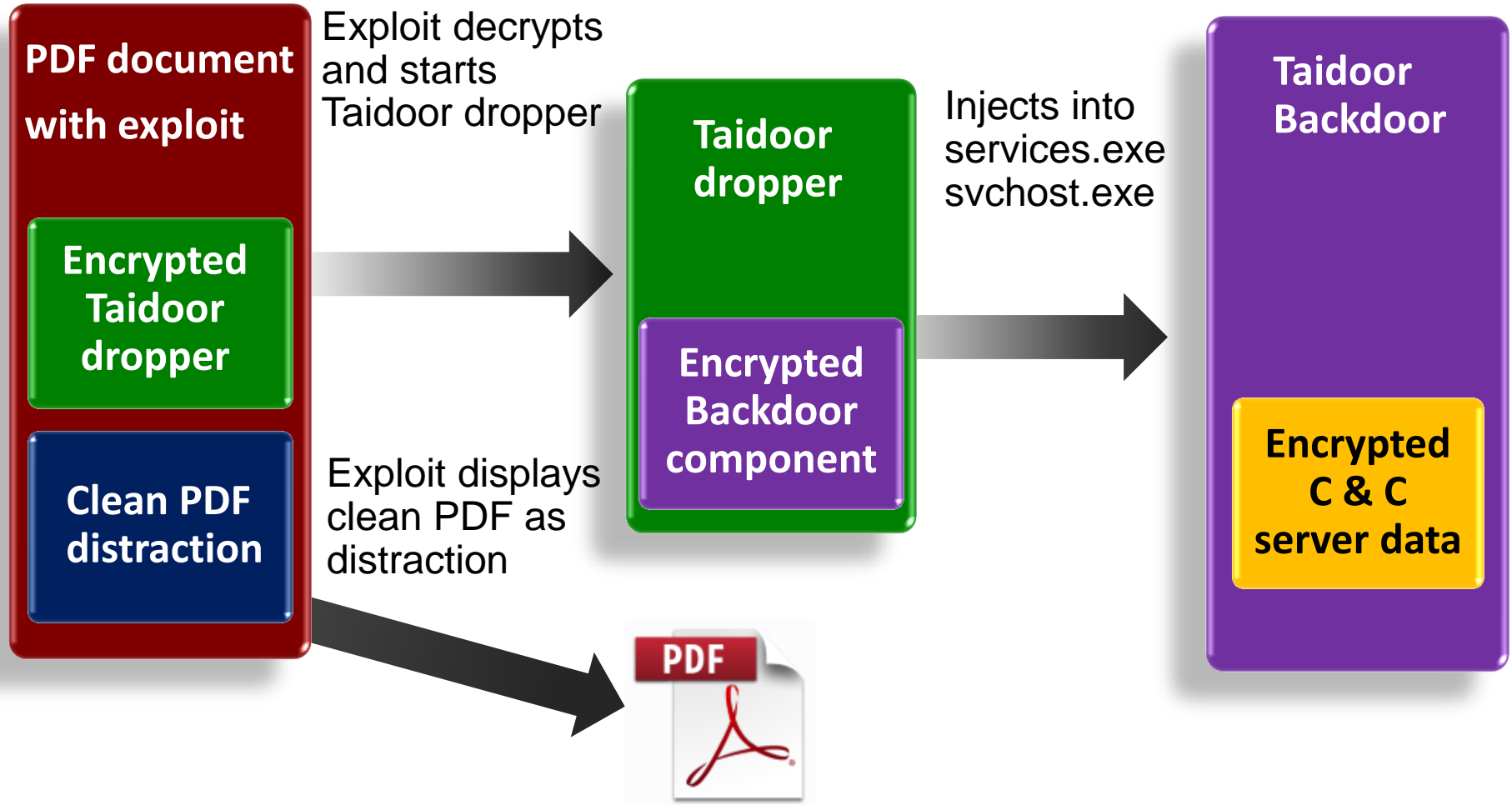
Incursion: Malware used

- The malware used is not always sophisticated!
 - Common malware can be as sophisticated
- Updated over the time of operation
- Some use stolen certificate to sign it

Malware used in simple attacks:	Attack:
• Poison Ivy – public Remote Access Trojan	Nitro
• Poison Ivy – public Remote Access Trojan	RSA breach
• VBS.Sojax – simple backdoor	Lucky Cat
• Taidoor – simple HTTP backdoor	Taidoor



Foothold: Infection with Trojan.Taidoor



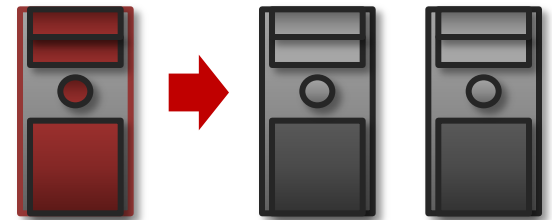
Discovery



Discovery

Expand foothold at target - searching for the data

- Plan next steps / next local infections
- May depend on commands from C&C server
- Use stolen credentials / information



Protection: IPS, strong authentication, SIM, segmentation



Manual Discovery: Example Taidoor

- We recorded interactive sessions with honeypots

Commands received by Taidoor

[Ping]

[Set sleep interval to 1 second]

```
cmd /c net start
```

```
cmd /c dir c:\docume~1\
```

```
cmd /c dir "c:\docume~1\\recent" /od
```

```
cmd /c dir c:\progra~1\
```

```
cmd /c dir "c:\docume~1\\desktop" /od
```

```
cmd /c netstat -n
```

```
cmd /c net use
```

Manual Discovery: Example Sykipot

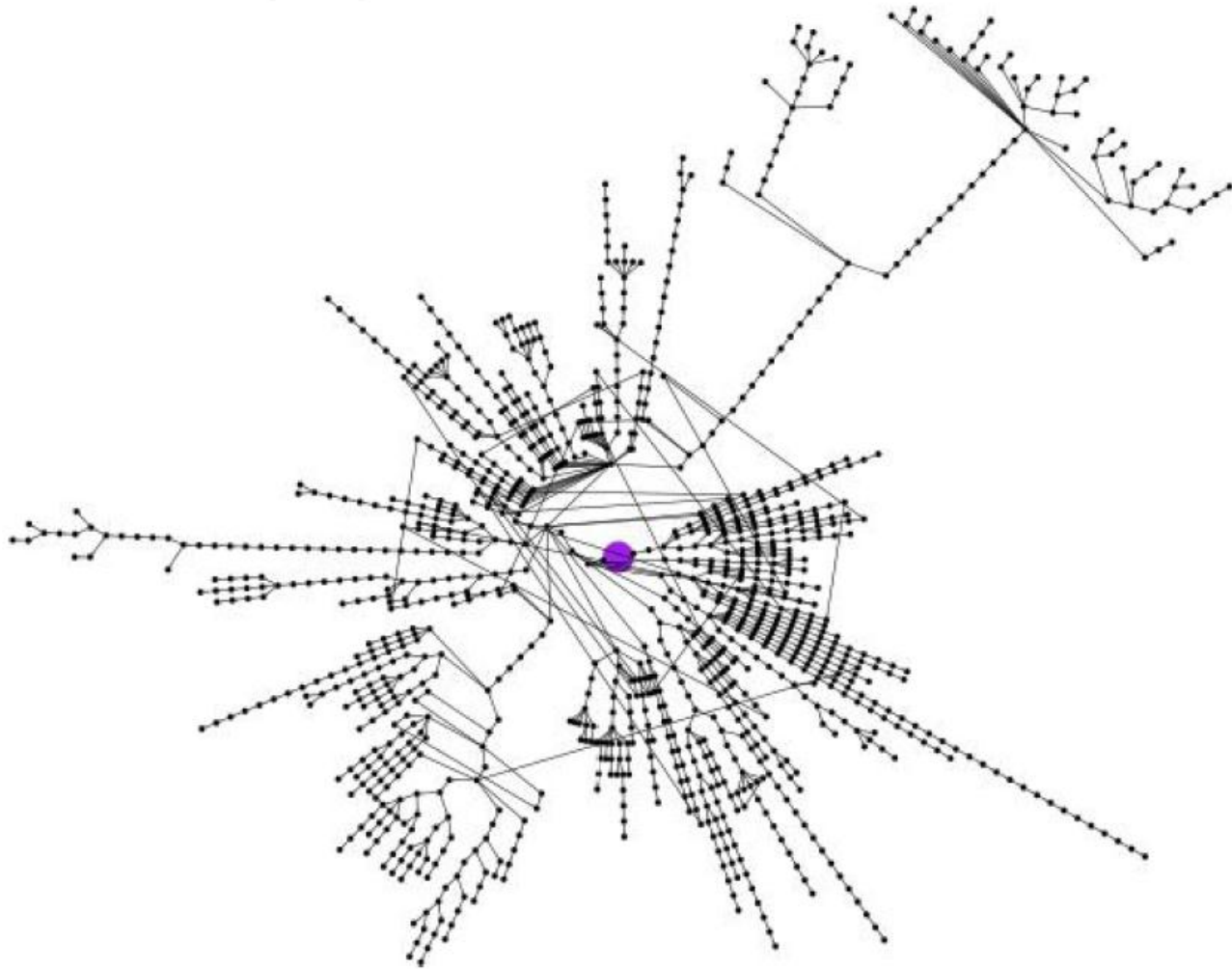
- They know what they are looking for

Commands received by Sykipot

```
ipconfig /all
netstat -ano
net start
net group "domain admins" /domain
tasklist /v
dir c:\*.url /s
dir c:\*.pdf /s
dir c:\*.doc /s
net localgroup administrators
type c:\boot.ini
systeminfo
```



Stuxnet propagation after one initial infection



Capture



Capture

Grab the interesting data

- Can happen over years
- Gathered in central place or multiple locations
 - Obfuscate and/or encrypt
- Database & file servers are a common target

Protection: ACL & DLP can help protect your critical information



Capture: Example Flamer

- Steals everything and more
 - Documents, images, phone synchronizations, voice recordings, Bluetooth data, screenshots, credentials, ...
- Filter on metadata, GPS, creation date, ...
- Stored encrypted on:
 - Local SQLite database
 - Files in %Temp% folder
 - Hidden on USB stick



Exfiltration



Exfiltration

Send the stolen information back to the attacker

- Drop server either rented, hacked or free hoster
- “smash & grab” attacks, if detection is likely

- Asymmetric encryption & SSH vs. HTTP posts
 - Both work, HTTP is often less suspicious

Protection: Filter outbound traffic, firewall, IPS, DLP, proxies



Exfiltration: Examples

- Most try it with HTTP posts (proxy aware)

Method used for exfiltration:	Attack:
• HTTP post with RC4 encrypted data	Taidoor
• HTTP/S post of JPEG with AES encrypted data	Duqu
• HTTP with OneTimePad XOR data	Stuxnet
• HTTP post of compressed .cab files	Lucky Cat



How to Apply What You Have Learned Today

- Verify where your critical data is stored
- Verify who can access that data
- Verify that you are able to detect data extraction
- Add this scenario to your response plan



Summary

- Targeted attacks do happen!
- Not all attacks are sophisticated, but they are dangerous as well
- Stolen data can be used to prepare further attacks
- You need defense in depth



A nighttime photograph of a city skyline with illuminated skyscrapers. In the foreground, a multi-lane highway shows long-exposure light trails from cars, with white trails for headlights and red trails for taillights. A yellow diamond-shaped road sign is visible on the left side of the road. The text 'Thank you for your attention!' is centered in a white rounded rectangle with a yellow border.

Thank you for your attention!

