Symantec.

Targeted attacks:
How sophisticated are they really?

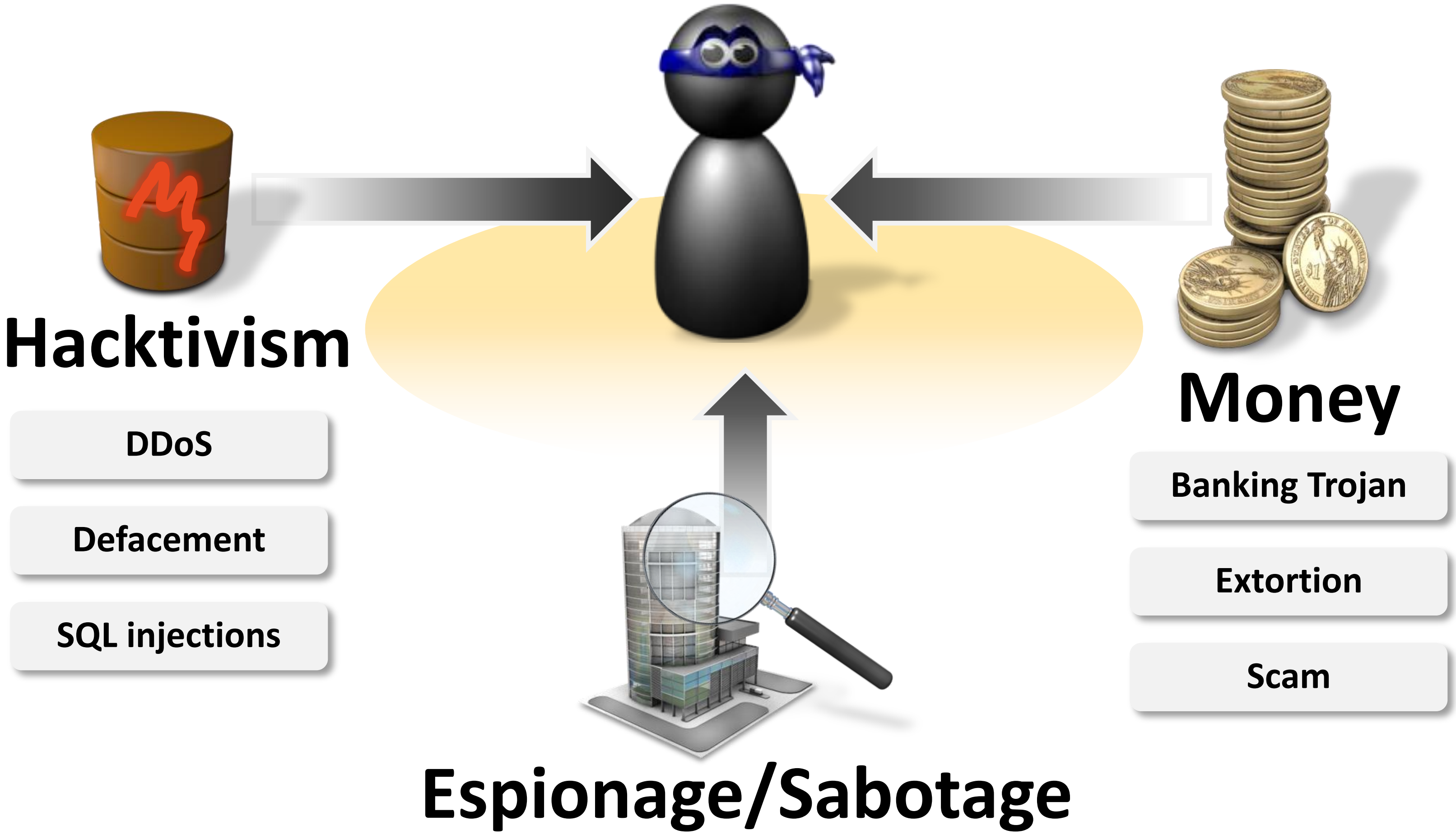
Candid Wüest

@threatintel

Threat Researcher @ Symantec Security Response

10:40 – 11:05

Different motives – Different attacks



Hacktivism

- DDoS
- Defacement
- SQL injections

Money

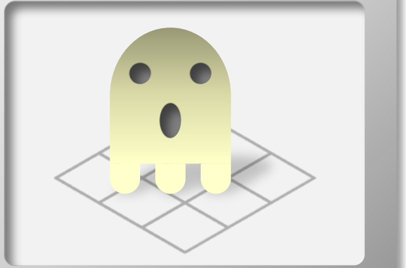
- Banking Trojan
- Extortion
- Scam

Espionage/Sabotage

Press SPACEBAR once to quit or twice to save changes...

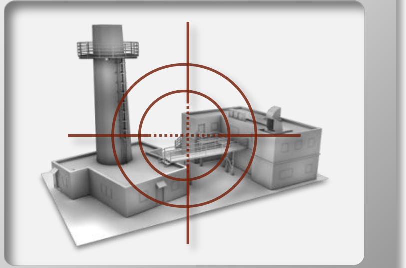
Many targeted attacks have been analysed…

Ghostnet



JUN 2008

W32.Stuxnet



JUN 2009

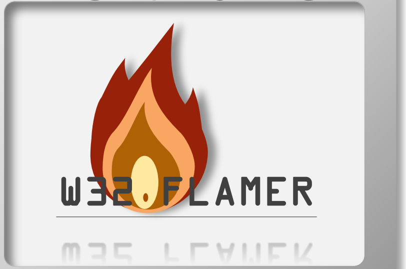
Night Dragon

FEB 2011

Elderwood

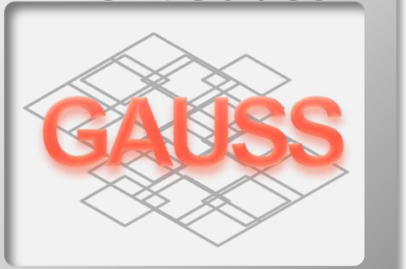
SEP 2012

W32.Flamer



MAY 2012

W32.Gauss



AUG 2012

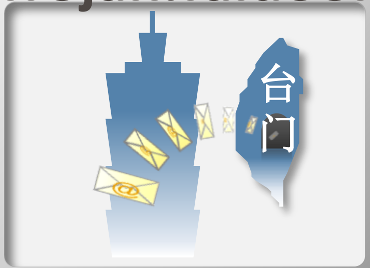
W32.Duqu

SEP 2011

Hydraq/Aurora

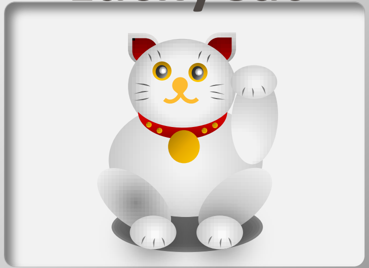
DEC 2009

Trojan.Taidoor



FEB 2012

LuckyCat



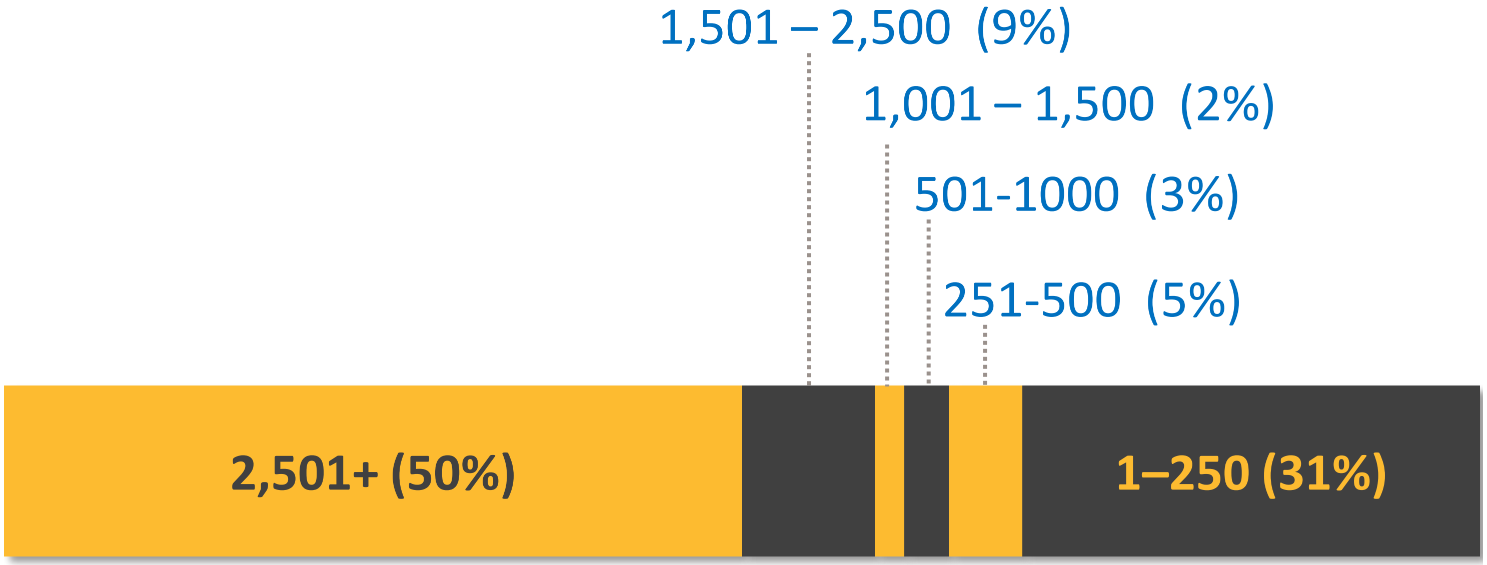
FEB 2012

Trojan.Jokra

MAR 2013

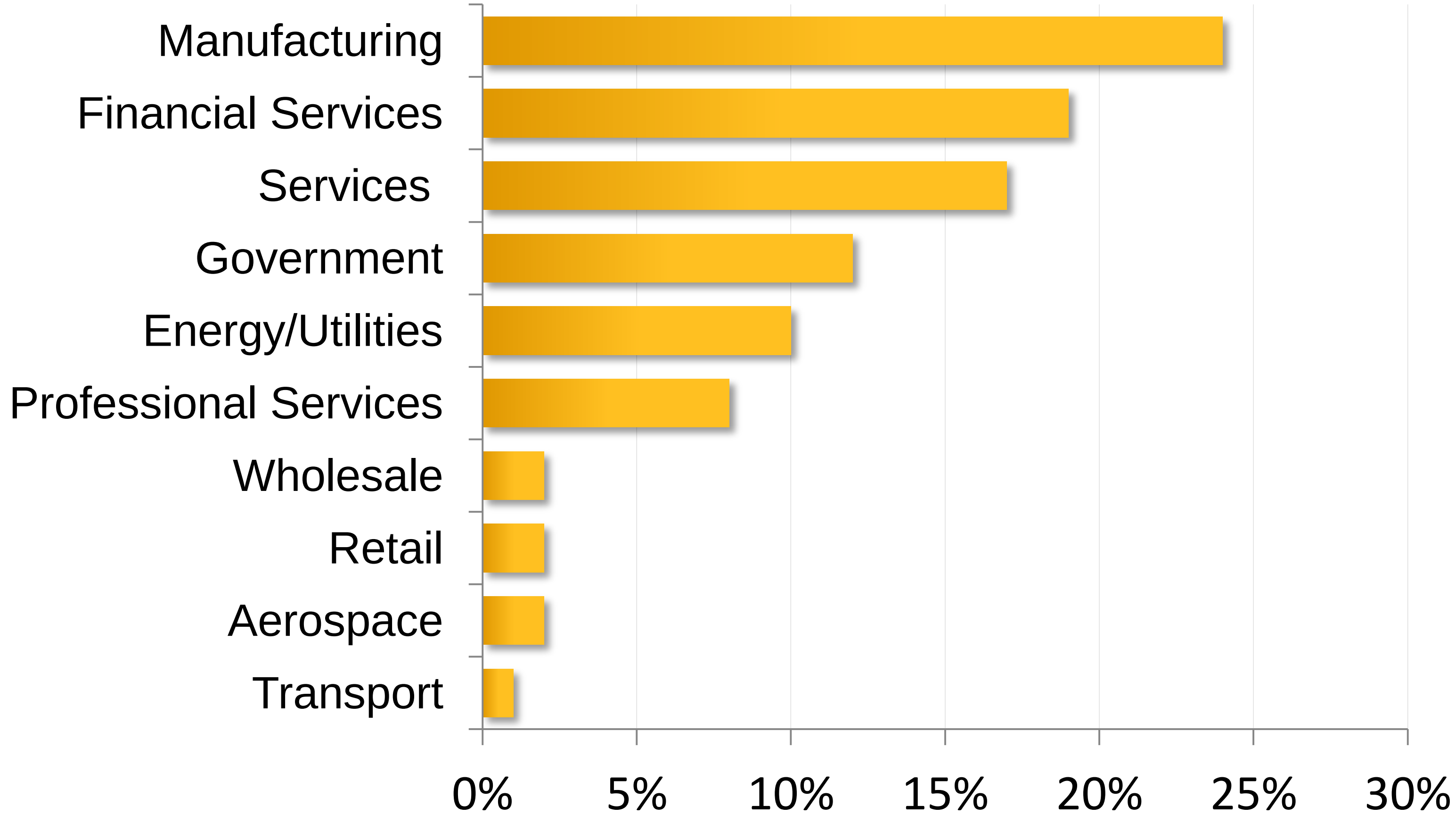
Size doesn‘t matter

- Small businesses may not be well protected
- Can be used as a stepping stone to get to larger organisations along the supply chain
- >230 targeted attacks / day in summer 2012



Number of employees per attacked company

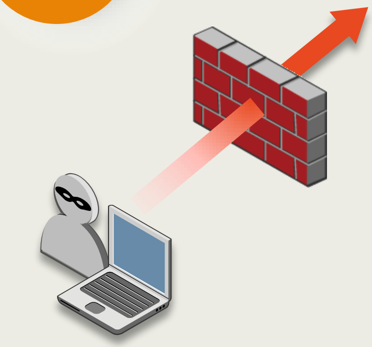
Most targeted sectors in 2012



The different phases

1 Reconnaissance

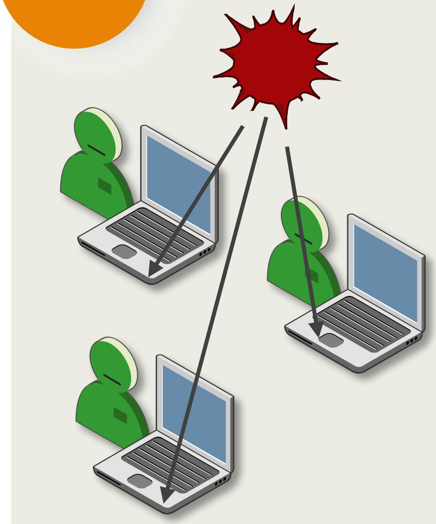
2



INCURSION

Attacker breaks into the network by delivering targeted malware to vulnerable systems and employees

3

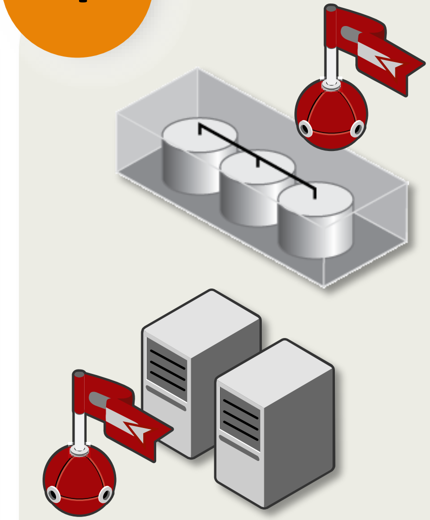


DISCOVERY

Hacker then maps organization's defenses from the inside

Creates a battle plan

4

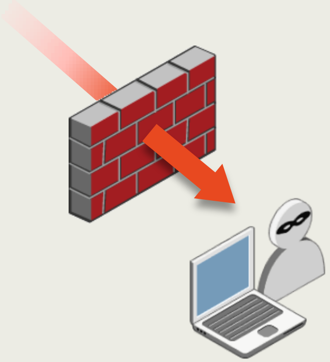


CAPTURE

Accesses data on unprotected systems

Installs malware to secretly acquire data or disrupt operations

5



EXFILTRATION

Data sent to enemy's "home base" for analysis and further exploitation/fraud

Classical attack vectors

Spear Phishing

Send an email to a person of interest

Watering Hole Attack

Infect a website of interest to your target user base and lie in wait for them

Alternatives:

USB sticks

Social engineering

Software vulnerabilities

Man-in-the-Middle attacks

Incursion: Malware used

- The malware used is not always sophisticated!
  - Common malware can be as sophisticated
- Bypassing AV signatures can be trivial
  - but there’s more than just static AV signatures

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

It’s true hard work never killed anybody, but why take the chance?

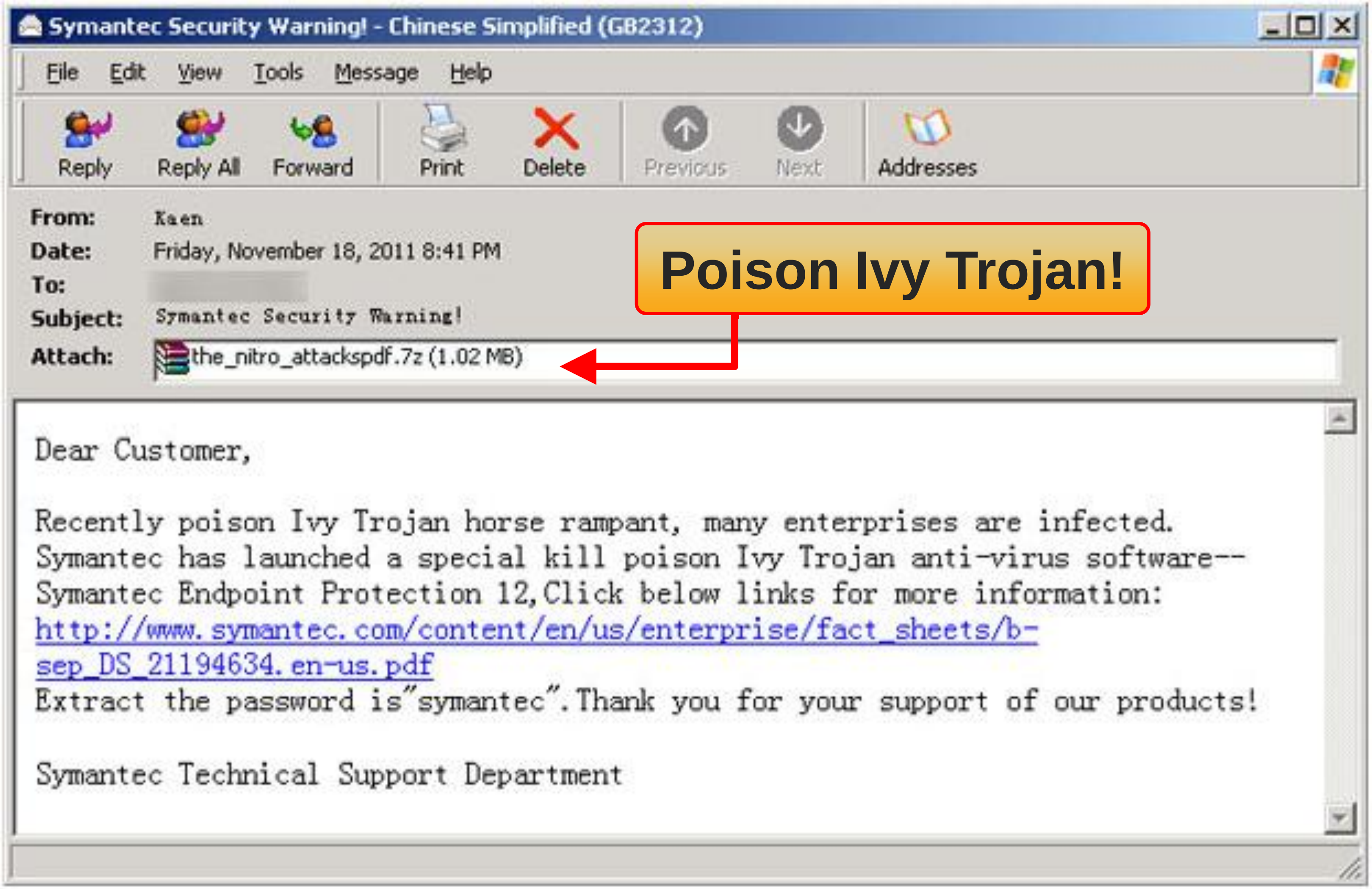
Some are indeed sophisticated

- Stolen Bit 9 signing key
- Stolen Adobe certificate
- Microsoft update certificate in Flamer
- South Korea: Trojan.Jokra distributed through software update

But even **SQL Injection** still works in many cases

– Old method, protection has been known for years

Nitro gang has a sense of humor



From: Kaen
Date: Friday, November 18, 2011 8:41 PM
To: [redacted]
Subject: Symantec Security Warning!
Attach: the_nitro_attackspdf.7z (1.02 MB)

Poison Ivy Trojan!

Dear Customer,

Recently poison Ivy Trojan horse rampant, many enterprises are infected. Symantec has launched a special kill poison Ivy Trojan anti-virus software--Symantec Endpoint Protection 12,Click below links for more information:
http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-sep_DS_21194634.en-us.pdf
Extract the password is"symantec".Thank you for your support of our products!

Symantec Technical Support Department

What happens if you get scared half to death twice?

Discovery: Manual Search Teams

- They know what they are looking for

Sykipot Honeypot Kommando

```
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
```

Taidoor Honeypot Kommando

```
[Ping]
[Set sleep interval to 1 second]
cmd /c net start
cmd /c dir c:\docume~1\
cmd /c dir
   "c:\docume~1\<CurrentUser>\recent" /od
cmd /c dir c:\progra~1\
cmd /c dir
  "c:\docume~1\<CurrentUser>\desktop" /od
cmd /c netstat –n
cmd /c net use
```

Exfiltration

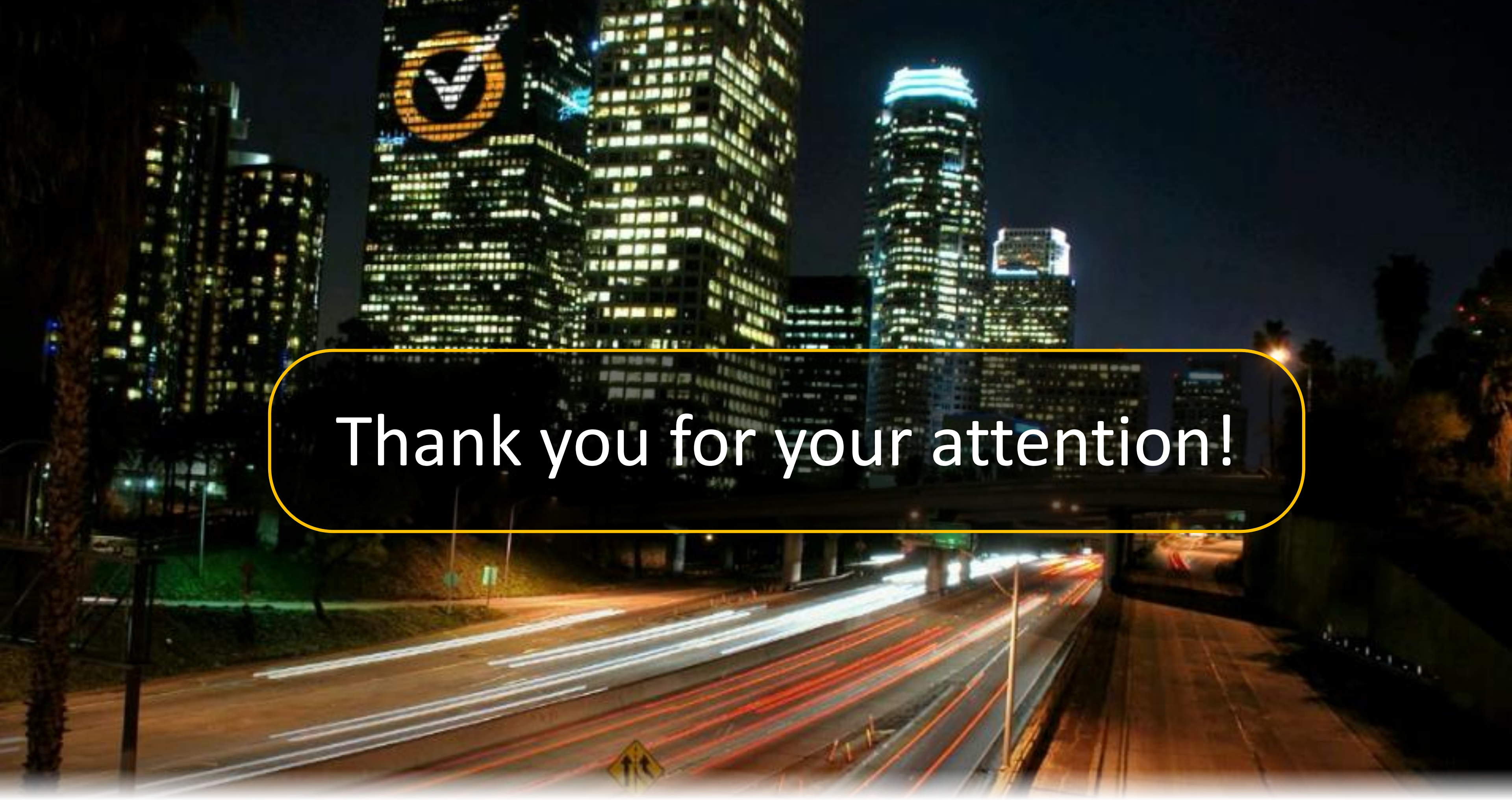
- Most try it with HTTP/S posts (proxy aware?!)
- Simple encryption or obfuscation of traffic (XOR, RC4,AES,…)
- Drop server either rented, hacked or free hoster
  - often cascaded proxies that will be wiped

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

Summary

- Depending on the motivation, the attack method might vary
- Targeted attacks do happen every day
- Not all attacks are sophisticated, but many are successfull
- Stolen information is reused in later attacks
- The person behind the malware makes the difference

Would you be able to detect outbound data streams?



Thank you for your attention!

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.