WORKING IN THE CYBERSECURITY AREA (CSIRT)

NEILO PERRIN-GANIER

SUMMER 2019

RICHEMONT

THE GROUP AT A GLANCE

*End March 2018

Founded in 1988

A leading luxury goods group

CHF 42.6 bn

Market capitalisation

€ 11 bn

Sales

€ 1.8 bn

Operating profit

OPERATING IN 4 BUSINESS AREAS

Jewellery Maisons

Cartier

Van Cleef & Arpels

Specialist Watchmakers

A. LANGE & SÖHNE GLASHÜTTE I/SA

BAUME & MERCIER MAISON D'HORLOGERIE GENEVE 1830

IWC SCHAFFHAUSEN

JAEGER-LECOULTRE

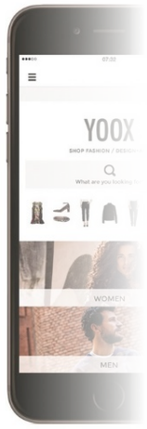
OFFICINE PANERAI FIRENZE 1860

PIAGET

ROGER DUBUIS

VACHERON CONSTANTIN GENÈVE

Online Distributors



WATCHFINDER&Co. THE PRE OWNED WATCH SPECIALIST

YOOX NET-A-PORTER GROUP

Other Businesses

ALAÏA PARIS

Chloé

dunhill

MONTBLANC

PETER MILLAR

PURDEY Gun & Rifle Makers LONDON 1814

SERAPIAN MILANO

RICHEMONT

«SECURITY» DEPARTMENT (HQ)

RICHEMONT

| Group Security

- **Physical security**

- **Risks**

- **Cyber Resilience**

  - **CSIRT (C**omputer **S**ecurity **I**ncident **R**esponse **T**eam**)**
  - **Risks**
  - **Infrastructures**
  - **Architects**

MISSIONS & INTERESTING CASES

RICHEMONT

MISSIONS

Incident response

- Detection → Centralisation → Treatment → Containment
  - Identification
    - Mail
    - Malware
  - Playbooks (tasks to do)

CSIRT
RICHEMONT
| Group Security

ONE INTERESTING CASE

Incident response

- Partner breached (or at least their mailbox)
- Hackers used the same templates as before (legit ones)
- Attached PDF with redirected link (O365)
- **GOAL** : Credentials steeling

CSIRT
RICHEMONT
| Group Security

OneDrive

You've received a secured doc via OneDrive, download or click on the View Document button below to view the document online.

PDF

P.D. (2.36 MB)

View Document

ONE INTERESTING CASE

Incident response

What we did :

- Blocked link and MD5 of the malicious PDF
- Retrieved targets in the group
- Asked them to change their password

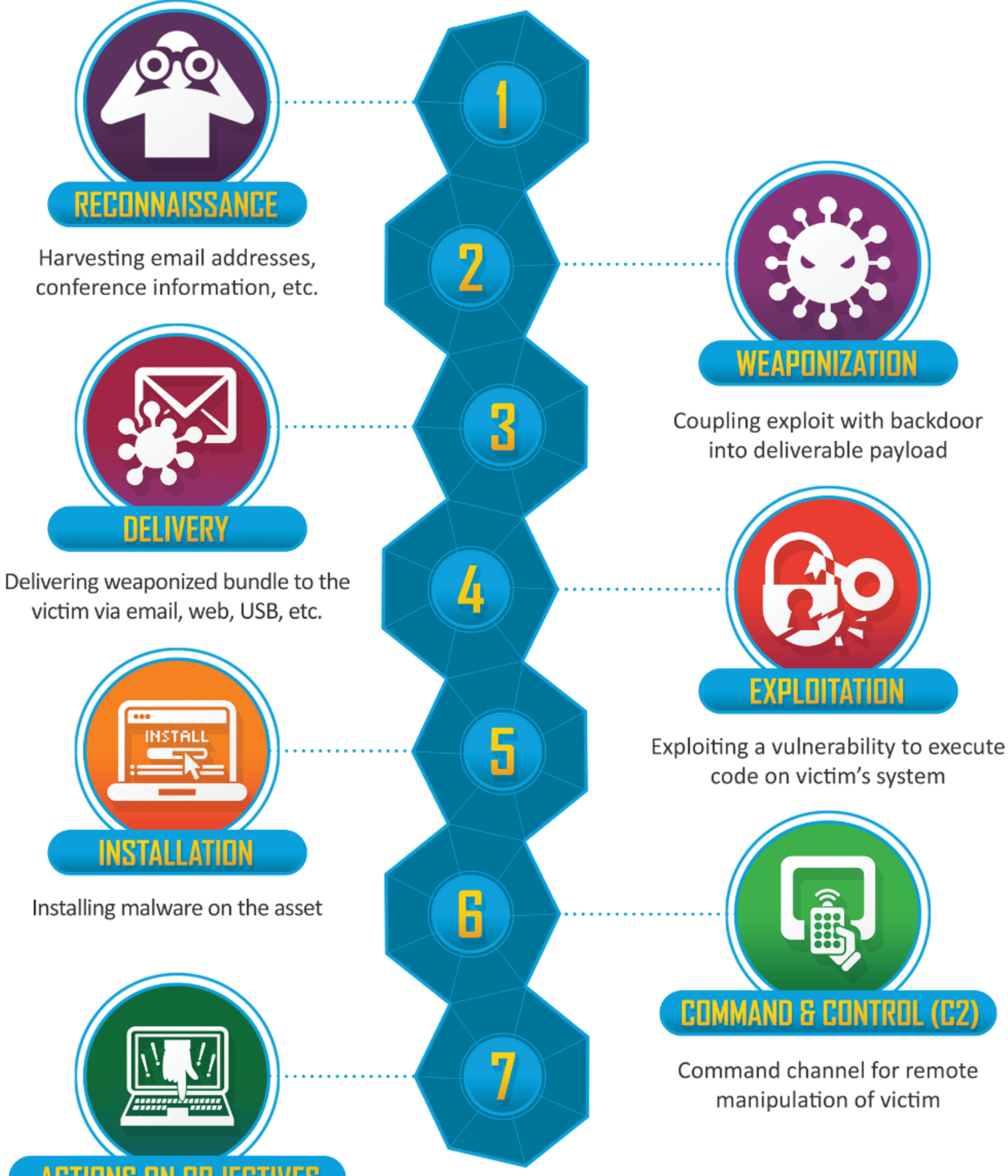
CSIRT
RICHEMONT
| Group Security

MISSIONS

Red team

- Take the place of a hacker and attack your own system
- Reconnaissance / Pentest / Exploit (entire killchain)
- Red team <=> Blue team
- Try to find any weakness

CSIRT
RICHEMONT
| Group Security


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

ONE INTERESTING CASE

Red team

Reconnaissance :

- Starting point : a simple DNS like "unige.ch"
- Extend and find sub-domain or related ones
- Tools : Amass, Osmedeus, Recon-ng, …
- Data base for pentest & ports scan

CSIRT
RICHEMONT
| Group Security

THANKS FOR YOU ATTENTION