ANALYZING AN OFF-THE-SHELF SURVEILLANCE SOFTWARE

HACKING TEAM CASE STUDY

Friday 2nd June, 2017

Stanislav Špaček

Pavel Čeleda, Martin Drašar,
Martin Vizváry

Introduction

Hacking Team Story

- Began as a security services provider in 2003
- Founders had previous experience with spyware development
- Recently develops tools for “offensive security”

Remote Control System Galileo (RCS)

- System for targeted surveillance of individuals
- Available exclusively to the governmental agencies
- System details were not released to the public

The Hacking Team Data Leak

Data Leak

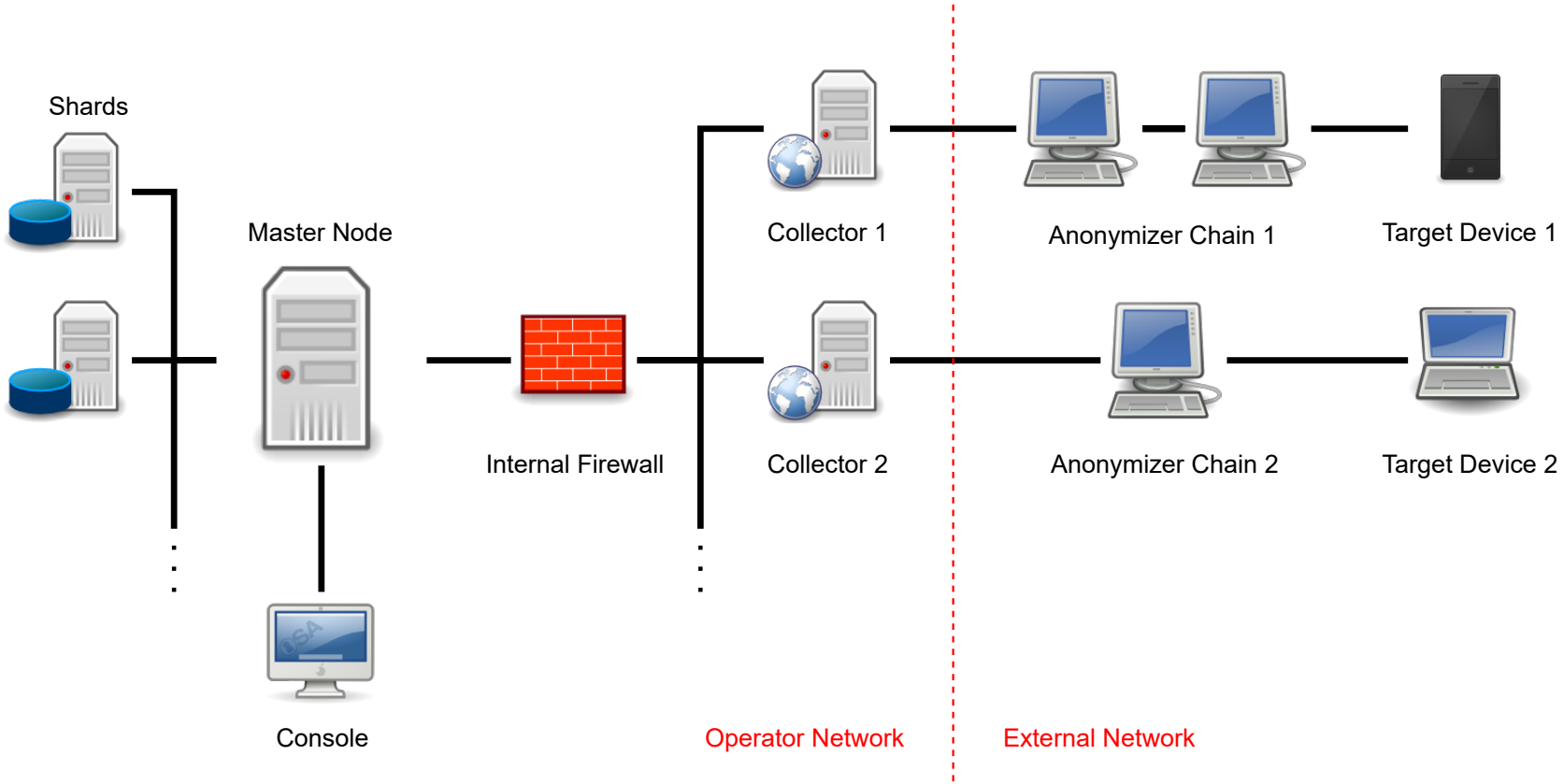
- Carried out by an unknown hacker in July 2015
- RCS and full documentation was made public

Research Objectives

- Analyze RCS functions and processes
- Run the system in KYPO cyber range
- Evaluate short and long term impact of the data leak

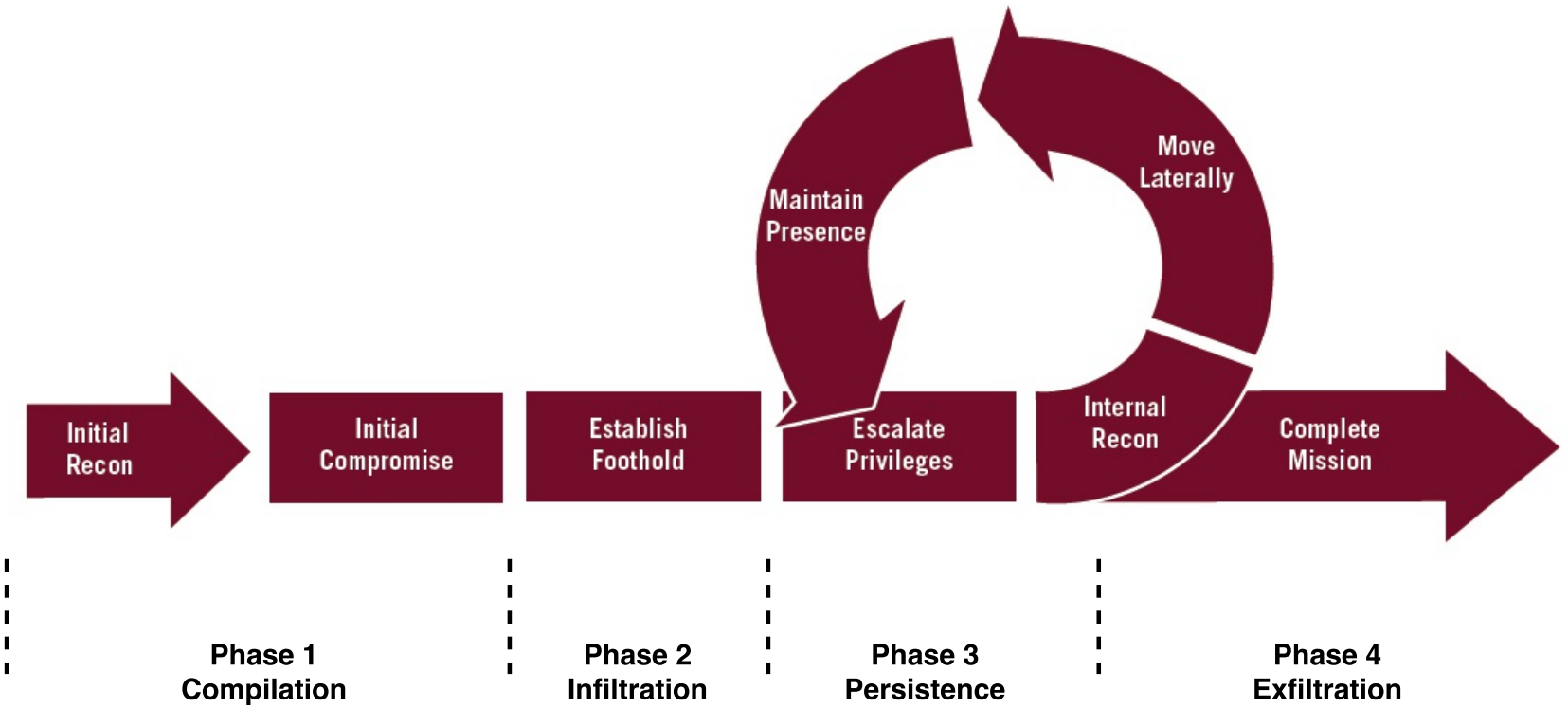
Remote Control System Galileo

Architecture



CSIRT-MU

APT x RCS Surveillance Operation Lifecycle

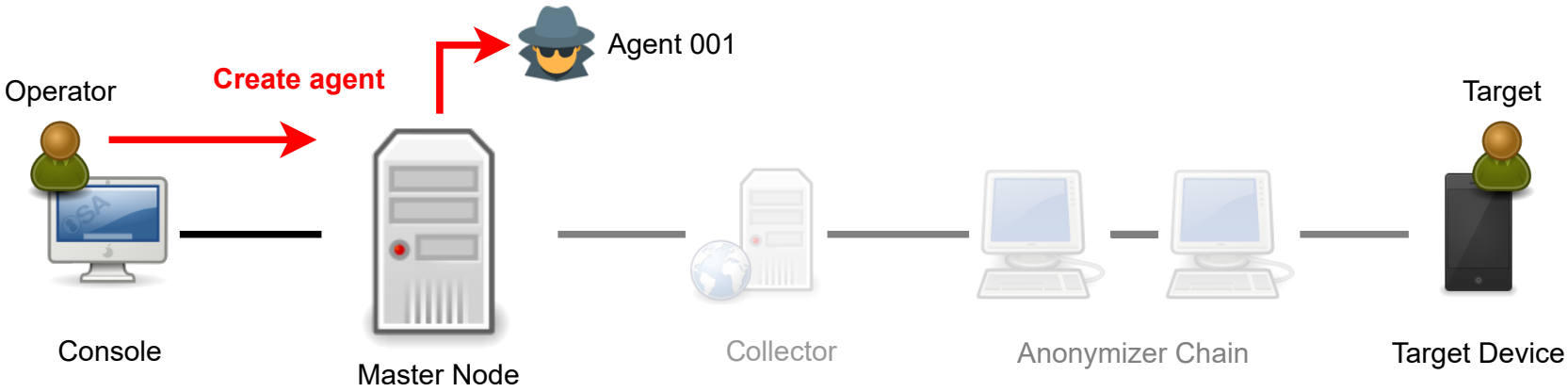


Mandiant, APT1: Exposing One of China's Cyber Espionage Units

CSIRT-MU

Surveillance Operation

Phase 1 – Compilation



- Requires target device specification (type, OS)
- *Agent* — spyware tailored for a specific target device

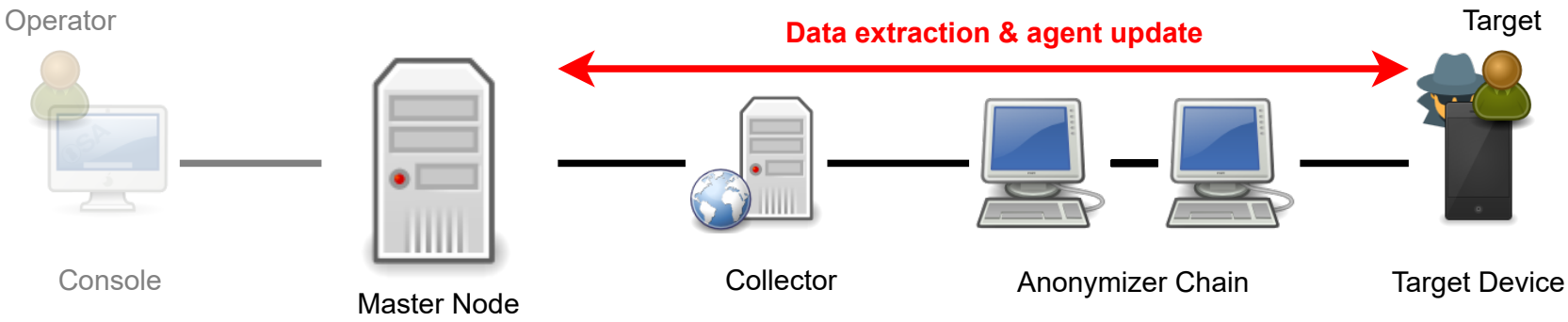
CSIRT-MU

Phase 2 – Infiltration

- Depends on chosen infection vector
- Usually carried out “outside” the RCS

CSIRT-MU

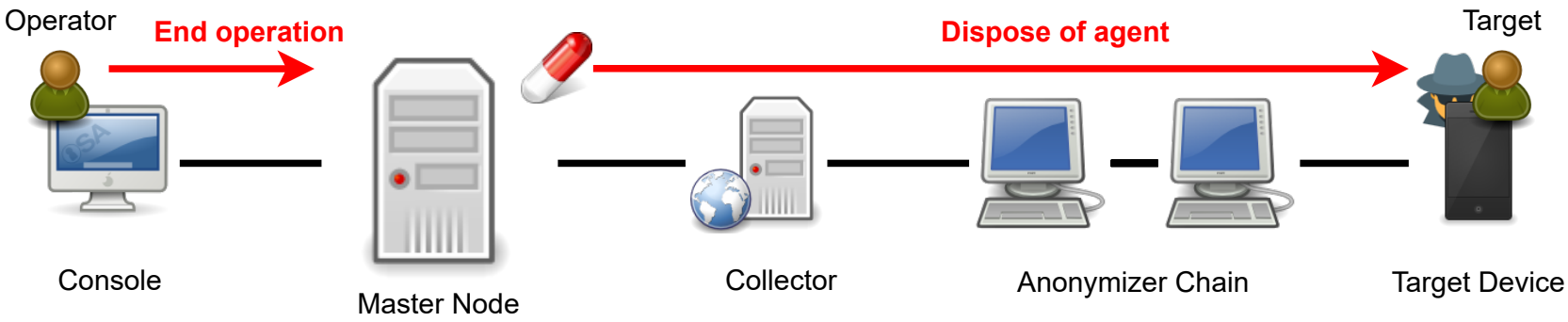
Phase 3 – Persistence



- The *agent* synchronizes at set intervals
- Extracted data is stored at the RCS database

CSIRT-MU

Phase 4 – Exfiltration



- The operation is terminated
- All *agents* are ordered to uninstall during next synchronization

CSIRT-MU

Novel Approaches in RCS

Frontend

Agent

- Properties adopted from known malware
  - Infection vectors – targeted malware
  - Surveillance functions – spyware
  - C&C communication – multilayered botnet
- Lacks deep customization options of APT malware
- Focused on stealth at the expense of function

Backend

Administrative Interface

- Every action available through point & click
- Exhaustive user documentation and system *wizards*

Consumer Support

- Updates to infection vectors, functions etc.
- Access to o-day exploits
- Hacking Team had a kill switch for each sold instance of RCS

Conclusion

Conclusion

Short-Term Effect

- No large misuse incidents were reported
- Contributed to Adobe Flash deprecation

Long-Term Effect

- Marginal – RCS adopted processes from existing malware
- Administrative interface – might make APT attacks widely accessible
- Support processes – used in advanced mass spread malware frameworks

THANK YOU FOR YOUR ATTENTION

www.kypo.cz

@csirtmu

Stanislav Špaček

spaceks@ics.muni.cz

UNIVERSITAS MASARYKIANA BRUNENSIS

ÚVT

CSIRT-MU