Vševidoucí Galileo

RNDr. Marian Kechlibar, PhD.
CircleTech, s.r.o.

Hacking Team (leak dat)

- 6. července 2015 je zveřejněno 400 GB dat uniklých z italské SW společnosti Hacking Team
  - E-mailové schránky.
  - Faktury a obchodní kontakty.
  - Zdrojové soubory špionážního systému RCS Galileo.
  - Používané exploity.

Jak se leak uskutečnil?

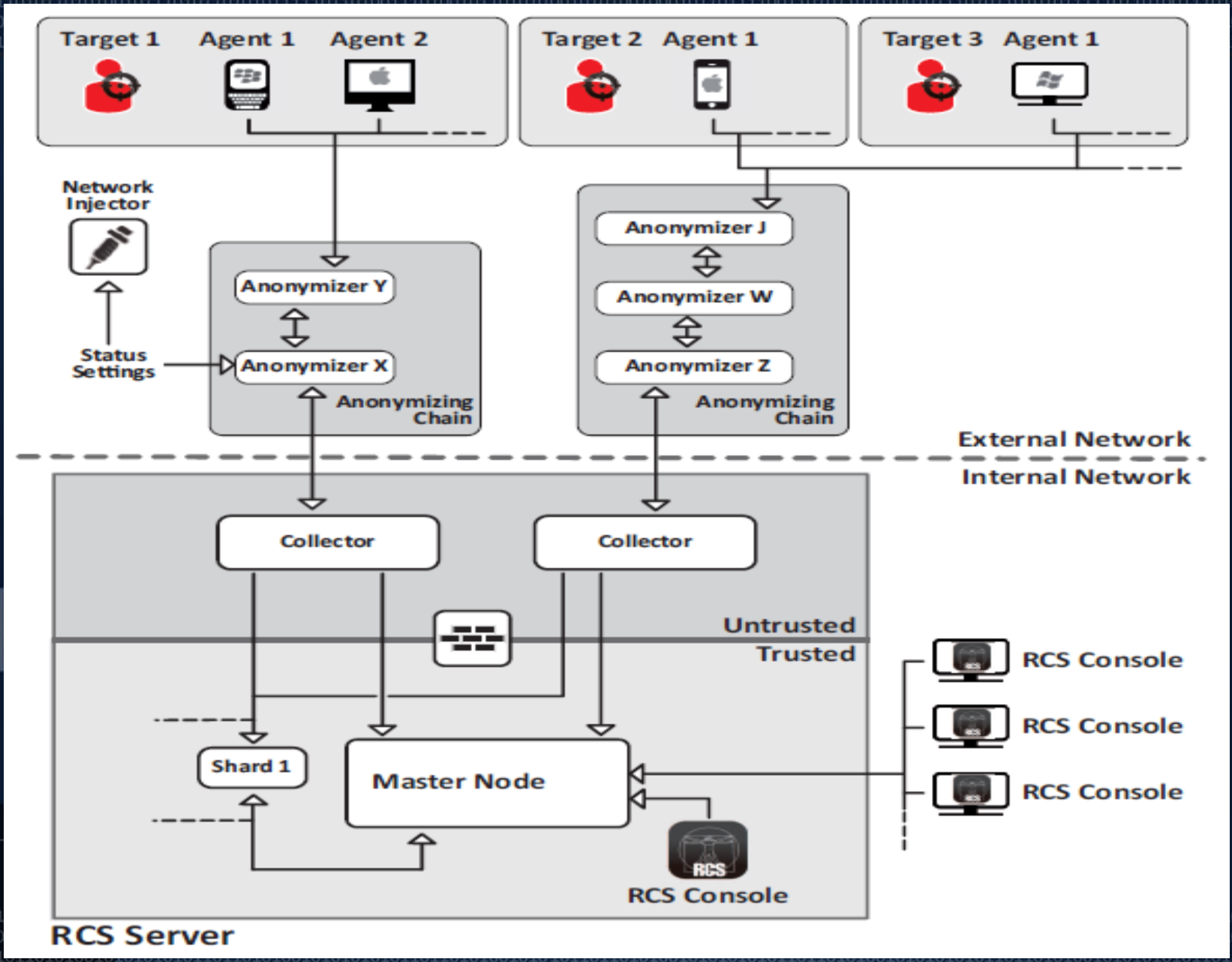
- Slabá hesla důležitých zaměstnanců:
  - Passw0rd,
  - P4ssword,
  - wolverine,
  - universo
  - HTPassword.
- Nejhorší hesla měl bezpečnostní šéf firmy Christian Pozzi.
  - Také na důležitých službách (žádné banality).

Významní zákazníci

- Zejména policejní a zpravodajské složky států:
  - Včetně diktatur (Súdán, Uzbekistán).
  - Včetně technicky rozvinutých zemí (USA).
  - Včetně Policie České republiky (Útvar zvláštních činností).
    - Nakoupeno přes firmu BULL s.r.o., celková cena pod 1 milion Eur.
- Seznam zákazníků potvrzuje vysokou technickou úroveň špionážního systému.

0-day exploity

- Na většině platforem byly základem 0-day exploity, které firma nakupovala přímo od výzkumníků.
  - Cena za jeden exploit v desítkách tisíc USD.
  - Výrazným zdrojem exploitů byl Adobe Flash (3).
  - Zajímavý pohled na trh s vulnerabilitami a jeho hlavní hráče (Singapur, Rusko, Francie).
  - Častá neochota výzkumníků spolupracovat se soukromou firmou.


Target 1
Agent 1
Agent 2
Target 2
Agent 1
Target 3
Agent 1
Network Injector
Status Settings
Anonymizer Y
Anonymizer X
Anonymizing Chain
Anonymizer J
Anonymizer W
Anonymizer Z
Anonymizing Chain
External Network
Internal Network
Collector
Collector
Untrusted
Trusted
Shard 1
Master Node
RCS Console
RCS Console
RCS Console
RCS Console
RCS Server

Systém v praxi

- Různé způsoby infekce cílového zařízení:
  - Sociální inženýrství („SMS s updatem“, přílohy e-mailů).
  - Přímá instalace (Silent Installer).
  - Vložení do nevinného programu (Melter).
  - Network Injector – aktivní protivník na síti, dedikované mezilehlé zařízení.
  - Speciální program na Google Store (BeNews)

A jak to v praxi vypadá…?

- Rozchodit systém z uniklých zdrojových kódů není příliš obtížné.
- Následně můžeme zprovoznit serverovou architekturu:
  - Master Node
  - Collector
  - Anonymizer
- … a začít infikovat koncové přístroje.