The Dark Side of the ForSSHe

Gaspare Ferraro

ICT Risk Assessment

University of Pisa
Master Degree in Computer Science

Pisa, July 17, 2019

Part I

Introduction

SSH

OpenSSH suite

The attackers

Operation Windigo

Part II

Common features of OpenSSH backdoors

Strings and code obfuscation

Credential stealing

Exfiltration methods

Backdoor mode

Part III

Backdoors families

OpenSSH backdoor galaxy

Chandrila

Bonadan

Kessel

Kamino

Part IV

Honeypot

Definition and goals

Honeypot structure and strategy

Observed interaction: Mimban

Observed interaction: Borleias

Part V

Compromission

Linux server market share

Operation Windigo summary

Operation Windigo damage

Part VI

Mitigation

Preventing compromise of SSH servers

Correct OpenSSH configuration

Check logs

Analyze network traffic

Detect compromised SSH tools

References