The Dark Side of the ForSSHe

A landscape of OpenSSH backdoors

Gaspare Ferraro

ICT Risk Assessment

University of Pisa
Master Degree in Computer Science

Pisa, July 18, 2019

Part I

Introduction

SSH

OpenSSH suite

Suite of secure networking utilities based on SSH protocol.

Coming by default in a large number of operating systems

Utilities:

- SCP, secure copy of files between two different hosts
- SFTP, secure file transfer program
- SSH, secure shell client
- SSHD, ssh server daemon
- keys utilities (SSH-ADD, SSH-AGENT, SSH-KEYGEN, SSH-KEYSCAN)

The attackers

Operation Windigo

Part II

Common features of OpenSSH backdoors

Strings and code obfuscation

Credential stealing

Exfiltration methods

Once credentials are stealed, attackers need to exfiltrate them:

Exfiltration by local file

Easy method: credentials are stored inside a file in the server,
hidden in filesystem (e.g.: .SO in /USR/BIN or .H in /USR/LOCAL/INCLUDE).
Problem: attackers needs to have a way back into the system.

Exfiltration by C&C server

Complex method: send credentials over the network instead of local file.
Problem: network communications are logged.
Some backdoor encrypt communication with a symmetric key.

Exfiltration by email

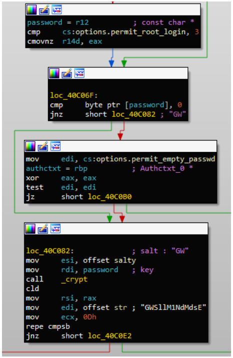
In some rare cases credentials are sent by email.
Problem: hardcode email address in the binary.

Backdoor mode

Permanent Method to connect back to the compromised machine,

with the following features:

- **Hardcoded password**,
- **Configuration and log**, TODO
- **Environment variables**, TODO
- **Hooked functions**, TODO



```
password = r12              ; const char *
cmp     cs:options.permit_root_login, 3
cmovnz  r14d, eax
```

```
loc_40C06F:
cmp     byte ptr [password], 0
jnz     short loc_40C082 ; "GW"
```

```
mov     edi, cs:options.permit_empty_passwd
authctxt = rbp              ; Authctxt_0 *
xor     eax, eax
test    edi, edi
jz      short loc_40C0B0
```

```
loc_40C082:                 ; salt : "GW"
mov     esi, offset salty
mov     rdi, password   ; key
call    _crypt
cld
mov     rsi, rax
mov     edi, offset str ; "GWSllM1NdMdsE"
mov     ecx, 0Dh
repe cmpsb
jnz     short loc_40C0E2
```

Backdoor password verification

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

Conclusion

References