The Dark Side of the ForSSHe

A landscape of OpenSSH backdoors

Gaspare Ferraro

ICT Risk Assessment

University of Pisa
Master Degree in Computer Science

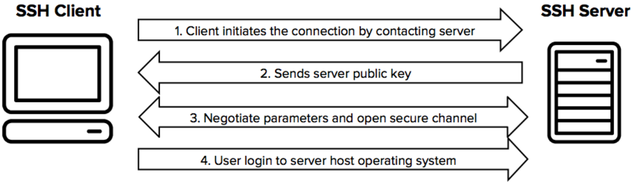
Pisa, July 20, 2019

Part I

Introduction

SSH

Secure **Sh**ell, protocol for secure remote login and other secure network services over an insecure network.


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system

Simplified setup flow (source: ssh.com)

Developed in 1995 in response to a hacking incident, today standard protocol for secure operations.

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)

Operation Windigo

Large and sophisticated operation started in 2011 and discovered after 3 years.

The operation has compromised linux servers in order to steal SSH credentials, redirect web traffic and send spam message.

Three different components of the operations:

- **Ebury, OpenSSH backdoor** used to gain full access, steal credentials and keep control of the servers.
- Cdorked, an HTTP backdoor used to redirect traffic and a modified DNS server to resolve arbitrary IP addresses.
- Calfbot, a Perl script used to send spam.

Results:

- highly portable malicious modules were developed in order to cover as many system as possibile.
- 25,000 unique servers compromised.
- 500,000 visitors per day redirected to malicious websites.
- 35,000,000 spam email sent.

Post-operation analysis

Post-operation analysis lead ESET to extend coverage about OpenSSH backdoors.

After months of research and data collection, ESET grouped a series of samples in 21 different OpenSSH malware families, 12 of them undocumented at the time of the paper.

ESET - IT security company

Malware were divided according to common features and cataloged by complexity and time of activity.

Part II

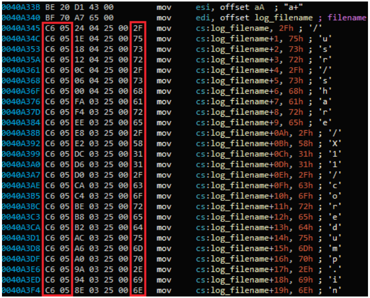
Common features of OpenSSH backdoors

Strings and code obfuscation

Attackers need a way to obfuscate strings and code of backdoor (such as filenames or directories).

XOR cipher: simplest method, encrypt the strings by xor the string with a key.

String stacking: construct strings directly in the stack in order to bypass simple string searched.



```
0040A33B BE 20 D1 43 00          mov     esi, offset aA  ; "a+"
0040A340 BF 70 A7 65 00          mov     edi, offset log_filename ; filename
0040A345 C6 05 24 04 25 00 2F    mov     cs:log_filename, 2Fh ; '/'
0040A34C C6 05 1E 04 25 00 75    mov     cs:log_filename+1, 75h ; 'u'
0040A353 C6 05 18 04 25 00 73    mov     cs:log_filename+2, 73h ; 's'
0040A35A C6 05 12 04 25 00 72    mov     cs:log_filename+3, 72h ; 'r'
0040A361 C6 05 0C 04 25 00 2F    mov     cs:log_filename+4, 2Fh ; '/'
0040A368 C6 05 06 04 25 00 73    mov     cs:log_filename+5, 73h ; 's'
0040A36F C6 05 00 04 25 00 68    mov     cs:log_filename+6, 68h ; 'h'
0040A376 C6 05 FA 03 25 00 61    mov     cs:log_filename+7, 61h ; 'a'
0040A37D C6 05 F4 03 25 00 72    mov     cs:log_filename+8, 72h ; 'r'
0040A384 C6 05 EE 03 25 00 65    mov     cs:log_filename+9, 65h ; 'e'
0040A38B C6 05 E8 03 25 00 2F    mov     cs:log_filename+0Ah, 2Fh ; '/'
0040A392 C6 05 E2 03 25 00 58    mov     cs:log_filename+0Bh, 58h ; 'X'
0040A399 C6 05 DC 03 25 00 31    mov     cs:log_filename+0Ch, 31h ; '1'
0040A3A0 C6 05 D6 03 25 00 31    mov     cs:log_filename+0Dh, 31h ; '1'
0040A3A7 C6 05 D0 03 25 00 2F    mov     cs:log_filename+0Eh, 2Fh ; '/'
0040A3AE C6 05 CA 03 25 00 63    mov     cs:log_filename+0Fh, 63h ; 'c'
0040A3B5 C6 05 C4 03 25 00 6F    mov     cs:log_filename+10h, 6Fh ; 'o'
0040A3BC C6 05 BE 03 25 00 72    mov     cs:log_filename+11h, 72h ; 'r'
0040A3C3 C6 05 B8 03 25 00 65    mov     cs:log_filename+12h, 65h ; 'e'
0040A3CA C6 05 B2 03 25 00 64    mov     cs:log_filename+13h, 64h ; 'd'
0040A3D1 C6 05 AC 03 25 00 75    mov     cs:log_filename+14h, 75h ; 'u'
0040A3D8 C6 05 A6 03 25 00 6D    mov     cs:log_filename+15h, 6Dh ; 'm'
0040A3DF C6 05 A0 03 25 00 70    mov     cs:log_filename+16h, 70h ; 'p'
0040A3E6 C6 05 9A 03 25 00 2E    mov     cs:log_filename+17h, 2Eh ; '.'
0040A3ED C6 05 94 03 25 00 69    mov     cs:log_filename+18h, 69h ; 'i'
0040A3F4 C6 05 8E 03 25 00 6E    mov     cs:log_filename+19h, 6Eh ; 'n'
```

String stacking in a binary

Credential stealing

Various methods to steal users credential on both sides.

Client

Modify functions on client to log password on log-in such:

USERAUTH_PASSWD, Authenticates a session with username and password.

SSH_ASKPASS, Pass-phrase dialog.

Server

Modify functions on server to log password on request such:

AUTH_PASSWORD, Tries to authenticate the user using password.

SSHPAM_RESPOND, Tries to authenticate the user with PAM (Pluggable authentication modules).

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,

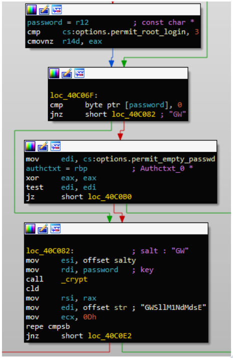
with the following features:

Hardcoded password, compare client password with a hardcoded password.

Configuration and log, change daemon configuration to permit full access and disable logging features in order to not leave traces on the system.

Environment variables, change environment variables such as HISTFILE.

Hooked functions, modify all functions for loggin and debugging.



```
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
```

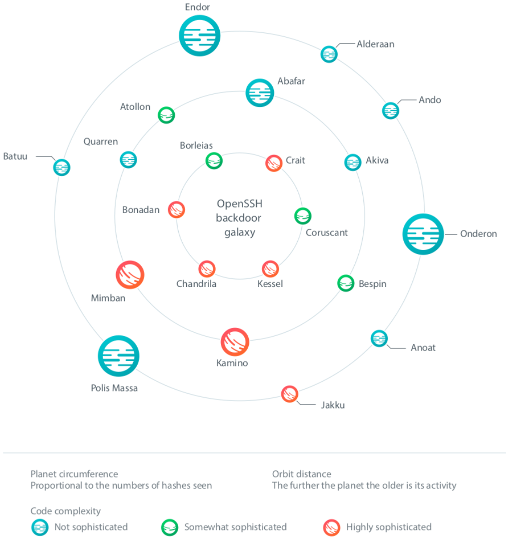
```
loc_40C082:                 ; salt : "GW"
mov     esi, offset salty
mov     rdi, password   ; key
call    _crypt
cld
mov     rsi, rax
mov     edi, offset str ; "GWSl1M1NdMdsE"
mov     ecx, 0Dh
repe cmpsb
jnz     short loc_40C0E2
```

Backdoor password verification

Part III

Backdoors families

OpenSSH backdoor galaxy



OpenSSH backdoor families according to ESET research

Chandrila

Save authentication method, username and password base64-encoded.

Exfiltration of credentials via local file or sent via UDP to a C&C server.

Distinctive feature: **can receive commands through the SSH password**. Two password are hardcoded in the backdoor: one to login in the server and another to execute commands, by appending data to the password.

Powerful backdoor mode as attacker can execute command without a shell.

Bonadan

Backdoor fork a new thread inside the main function: this thread periodically calls two functions and pause for five minutes.

First function check if there is any **cryptocurrency miner** installed on the system and removes it.

Second function connect to the C&C server and send several informations about the host over UDP (such as current username, OS version, external IP address, CPU and RAM models, speed of the miner).

Backdoor receive an answer from the C&C server that can containing a specific command like: create a shell, execute a command on machine, updates the configuration, launch a cryptocurrency mining module.

The backdoor mines the **Monero cryptocurrency** as part of a mining pool.

Problem: need to store wallet informations inside the server.

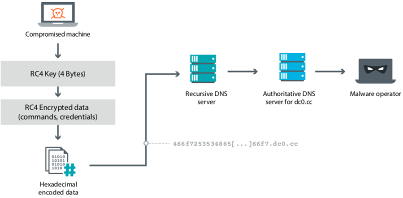
Kessel

Most advanced and recent between all the families. This backdoor includes two main features: a bot functionality and credentials stealing.

Bot feature: a bot is launched at the beginning of the OpenSSH main function, generate an ID based on MAC address, collect system information then starts two threads.

First thread periodically send encrypted informations to a C&C server and eventually create a reverse shell with a specified machine. Second thread repeatedly queries a TXT records in a custom DNS server to get commands.

Credential stealing: reimplements two malicious functions in SSH daemon (SSH_LOGIN and USER_AUTH_PUBKEY) to steal remote host/username, password and local username (or private/public key). Exfiltrate stolen credentials using HTTP, TCP or DNS protocol.


Compromised machine
RC4 Key (4 Bytes)
RC4 Encrypted data (commands, credentials)
Hexadecimal encoded data
466f7253534865[...]66f7.dc0.cc
Recursive DNS server
Authoritative DNS server for dc0.cc
Malware operator

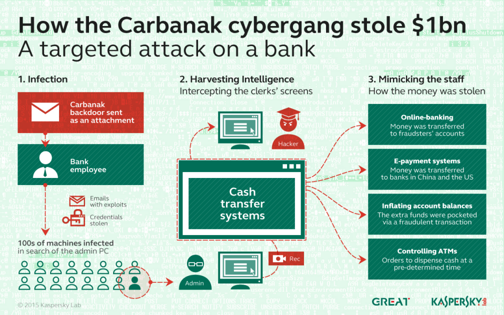
DNS exfiltration schema

Kamino

First variant of this backdoor already seen in 2013 (as documented in **[3]**).

Used together with an Apache module called DarkLeech to redirect internet traffic.

After few years the same backdoor was used again to attack Russian Banks by a group known as Carbanak, resulting in ∼900 million dollars



How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

Cash transfer systems

3. Mimicking the staff

How the money was stolen

Online-banking: Money was transferred to fraudsters' accounts

E-payment systems: Money was transferred to banks in China and the US

Inflating account balances: The extra funds were pocketed via a fraudulent transaction

Controlling ATMs: Orders to dispense cash at a pre-determined time

Carbanak attack (source: Kaspersky**[7]**)

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

[1] **The Dark Side of the ForSSHe, ESET**
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf

[2] **The Dark Side of the ForSSHe, ESET**
https://www.welivesecurity.com/2018/12/05/dark-side-of-the-forsshe/

[3] **Linux/SSHDoor.A Backdoored SSH daemon that steals passwords, ESET**
https://www.welivesecurity.com/2013/01/24/linux-sshdoor-a-backdoored-ssh-daemon-that-steals-passwords/

[4] **Operation Windigo, ESET**
https://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf

[5] **ESET discovers 12 previously undetected Linux backdoors, ESET**
https://www.eset.com/int/about/newsroom/press-releases/research/eset-discovers-12-previously-undetected-linux-backdoors/

[6] **Openssh backdoor used on compromised Linux servers**
https://www.randhome.io/blog/2016/08/01/openssh-backdoor-used-on-compromised-linux-servers/

[7] **Carbanak APT: The great bank robbery, Kaspersky**
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf