국내 모 제약회사 코로나 19 백신 연구 데이터 1.4TB 탈취, 제약 및 보험사 집중 타깃

RA 그룹 랜섬웨어

요약

1. 2023년 4월 새롭게 등장한 RA 그룹

- 한국과 미국의 보험사, 제약사가 주된 표적
- 초기에는 탈취 데이터 일부만 공개, 시간이 지나면 데이터 모두 공개

2. Babuk 랜섬웨어와 RA 그룹

- 소스코드가 유출된 Babuk 랜섬웨어를 개조
- RA 그룹은 '이중 협박' 전략 사용,
  피해자들에게 단 3일의 기한을 주어 심리적 압박을 강화하는 것이 특징
- RA 그룹의 정보 유출용 웹사이트에 피해 조직 데이터 공개 또는
  해당 사이트에서 피해 조직의 데이터를 직접 판매하기도 함

대응 방안

1. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
2. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션을 최신 형상으로 유지
3. PC 취약점을 주기적으로 점검, 보완
4. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단
6. OS나 어플리케이션은 최신 형상을 유지

목차

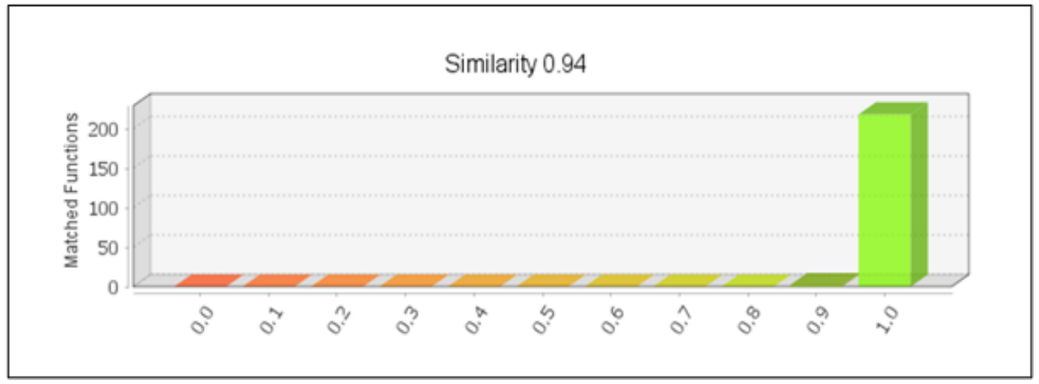
1. 개요

1.1 배경

[그림 1] 유출 사이트에 게시된 국내 모 제약회사

2023년 4월 28일, 국내 모 제약회사의 정부과제자료, 코로나19 연구자료 등의 데이터가 RA Group에서 운영하는 데이터 유출 사이트에 게시됐다.

RA Group은 2023년 4월부터 모습을 드러낸 새로운 랜섬웨어 그룹으로 현재까지 미국과 한국, 그리고 대만 기업을 차례로 공격했다.
이 그룹은 목적 달성을 위해 초기에는 탈취한 데이터의 일부만을 공개하여 피해자를 협박하다가 시간이 지나면 데이터를 모두 공개하는 전형적인 방식을 사용한다.
앞서 언급한 피해 기업인 국내 모 기업도 초기에는 데이터의 일부만 공개되었지만 현재는 데이터가 모두 공개되었다.

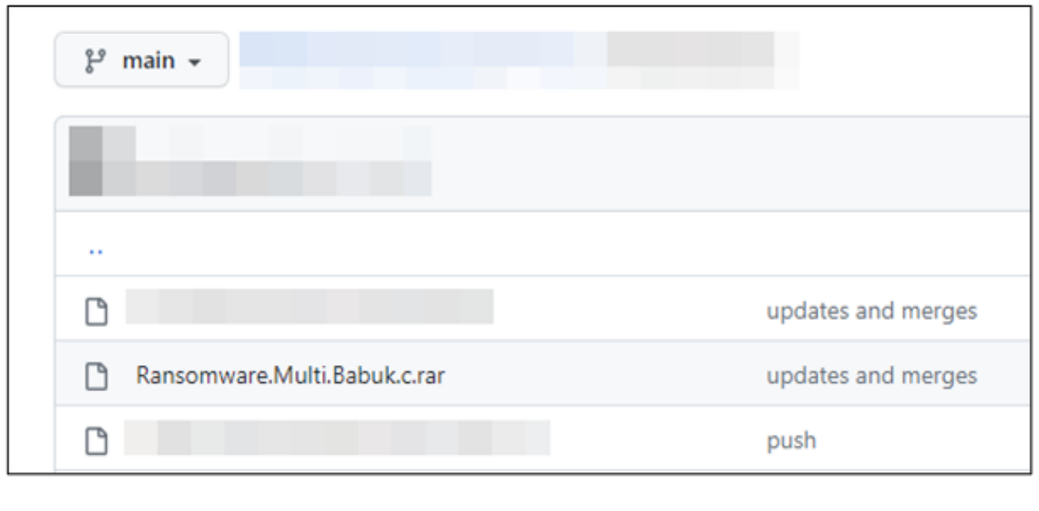


[그림 2] Babuk과 RA Group 간의 실행파일 유사도

RA Group 랜섬웨어의 샘플을 확보하고 분석하는 과정에서
Babuk과 유사한 코드 패턴, 동일한 문자열 등을 다수 확인할 수 있었다.
과거에 유포되었던 Babuk 랜섬웨어의 실행파일과 RA Group 랜섬웨어 실행파일의 유사도는 94%로
해당 랜섬웨어가 Babuk 랜섬웨어의 변종이라는 것을 알 수 있다.


```
text "UTF-8", 'C:\Users\attack\Desktop\Ransomware.Multi.Babuk.c\windo' ; PdbFileName
text "UTF-8", 'ws\x64\Release\e.pdb',0
```

[그림 3] RA Group 랜섬웨어에 포함된 심볼 파일 경로



[그림 4] GitHub에서 공유되고 있는 Babuk 소스코드

Babuk의 소스코드는 내부자로 추정되는 인물에 의해 해킹 포럼에서 최초로 공개됐다.
현재는 여러가지 경로로 소스코드를 구할 수 있는데,
심볼 파일 경로에 포함된 “Ransomware.Multi.Babuk.c”라는 폴더명으로 미루어 봤을 때,
공격자는 GitHub에서 Babuk의 소스코드를 입수한 것으로 추정된다.

등장 시기	악성코드 이름	특징 및 변경사항
2023.02	ESXiArgs	• VMware ESXi 대상 유포 • 암호 알고리즘을 RSA로 변경
2022.06	AstraLocker 2.0	• 윈도우즈 대상 유포 • Shielden 프로텍터로 실행파일 보호
2022.03	Pandora	• 윈도우즈 대상 유포 • UPX 패커로 실행파일 보호 • 분석 방지 기능 추가 (안티디버깅, ETW 우회 등) • 효율적인 암호화를 위해 IOCP 적용 • 암호 알고리즘을 RSA로 변경 • 현재는 다크웹 운영 중단
2022.01	NightSky	• 윈도우즈 대상 유포 • VMProtect 프로텍터로 실행파일 보호 • 암호 알고리즘을 AES, RSA로 변경 • 현재는 다크웹 운영 중단
2021.12	Rook	• 윈도우즈 대상 유포 • UPX 패커로 실행파일 보호 • 암호 알고리즘을 RSA로 변경 • 현재는 다크웹 운영 중단

[표 1] 과거의 Babuk 랜섬웨어 변종들

악성코드의 소스코드가 유출되면 공격자들은 이를 활용해 다양한 변종을 만들어 유포한다.
밑바닥부터 설계하고 코드를 작성하는 것보다는 잘 만들어진 것을 수정하는 방법이
비용적인 면에서 효율적이기 때문이다.
Babuk 랜섬웨어는 윈도우즈, NAS, VMware ESXi 등 플랫폼마다 소스코드가 별도로 존재하였기에
더더욱 공격자들에게 인기를 끌었고, 그 파급력 또한 거대했다.
[표 1]은 유출된 Babuk 소스코드를 이용해 랜섬웨어를 제작 및 유포했던 변종 목록이다.
본 보고서를 통해 RA Group 랜섬웨어가 기존과 비교하여 어떤 점이 바뀌었는지 알아본다.

1.2 파일정보

Name	e.exe
Type	PE64
SHA-256	3ab167a82c817cbcc4707a18fcb86610090b8a76fe184ee1e8073db152ecd45e
Description	RA Group 랜섬웨어 실행파일

[표 2] 악성코드 파일 정보

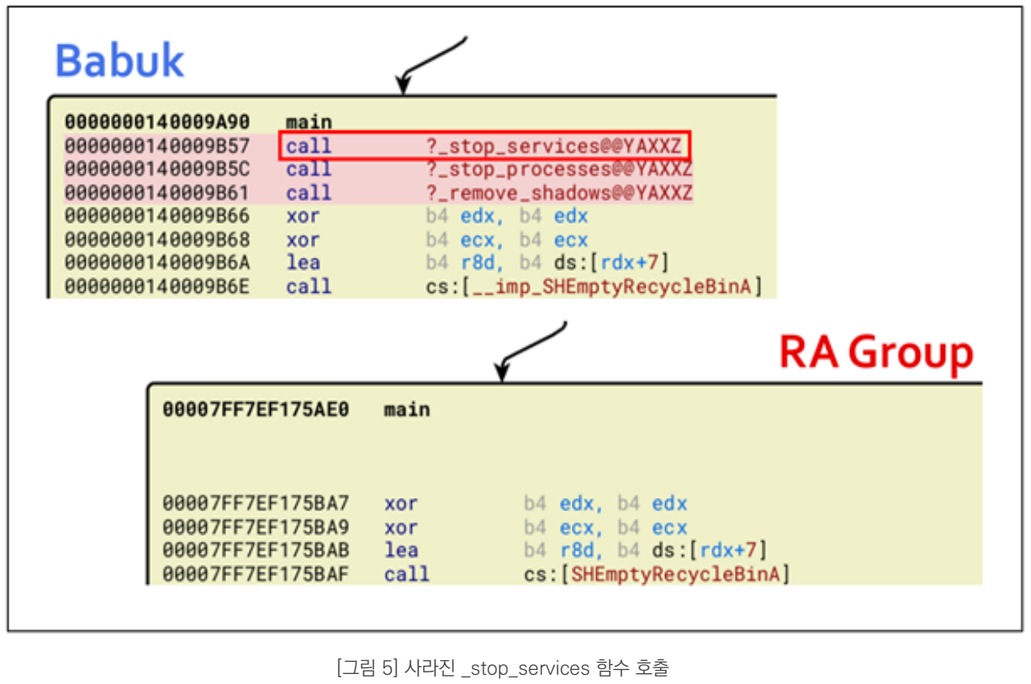
2. 분석

Babuk 랜섬웨어 (원본)	RA Group 랜섬웨어 (변종)
• 휴지통 비우기 • 서비스 강제 종료 • 프로세스 강제 종료 • 파일 암호화 • 랜섬노트 저장 • 볼륨 섀도 카피본 삭제	• 휴지통 비우기 • -서비스 강제 종료 (제거됨) • -프로세스 강제 종료 (제거됨) • +파일 암호화 (변경됨) • +랜섬노트 저장 (변경됨) • +볼륨 섀도 카피본 삭제 (변경됨)

[표 3] RA Group 랜섬웨어 변경점

RA Group은 필요에 따라 **[표 3]**과 같이 특정 기능을 제거하거나 수정하였다.
본 보고서는 RA Group 랜섬웨어에서 기존과 변함이 없는 기능은 제외시키고,
제거되거나 변경된 항목들만 포함하였다.

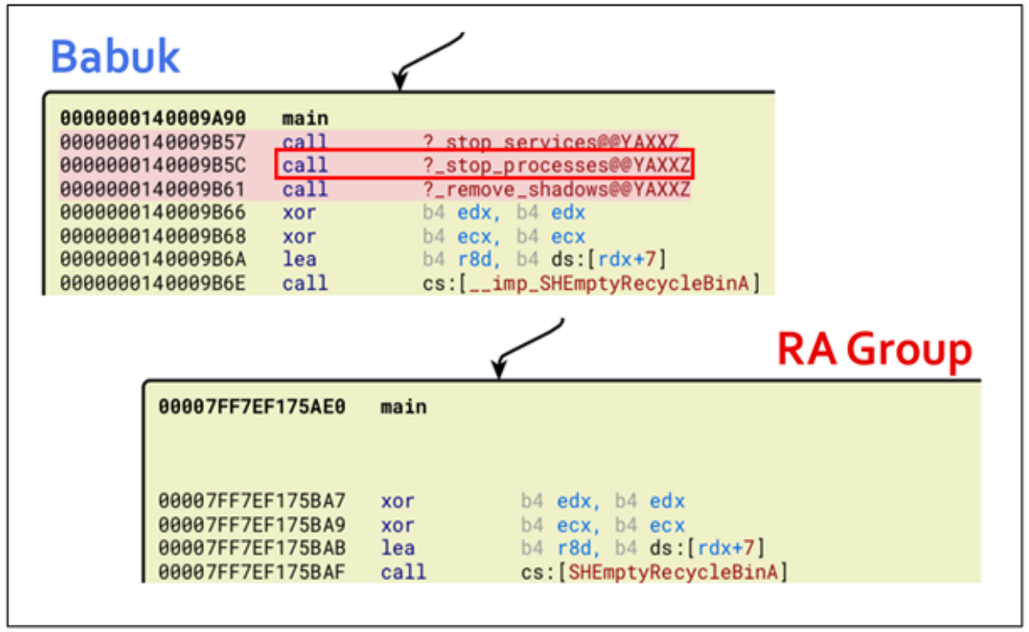
2.1 차이점 1: 서비스 강제 종료



[그림 5] 사라진 _stop_services 함수 호출

기존의 Babuk 랜섬웨어는 감염PC에서 동작 중인 서비스 중
블랙리스트에 등록된 서비스를 종료시키는 기능이 있었으나 RA Group에서는 그 기능이 제거되었다.
블랙리스트에 등록되어 있던 서비스의 개수는 총 44개였으며 백업 서비스들이 주로 포함되어 있었다.

2.2. 차이점 2: 프로세스 강제 종료



[그림 6] 사라진 _stop_processes 함수 호출

기존 Babuk 랜섬웨어는 감염PC에서 동작 중인 프로세스 중
블랙리스트에 등록된 프로세스를 강제로 종료시키는 기능이 있었으나
마찬가지로 RA Group에서는 제거되었다.
블랙리스트에 등록되어 있던 프로세스의 개수는 총 31개였으며,
읽기 또는 쓰기 공유 위반을 발생시킬 수 있는 데이터베이스,
문서 편집 프로그램 등이 주로 포함되어 있었다.

2.3. 차이점 3: 파일 암호화

```
; unsigned __int8 byte_7FF7EF17F150[32]
byte_7FF7EF17F150 db 0ABh, 0FAh, 6, 15h, 0, 13h, 2 dup(8Ah), 0D6h, 61h, 0A8h
                                        ; DATA XREF: sub_7FF7EF174000+66F↑o
                  db 99h, 0EEh, 0EBh, 8Eh, 0Ch, 1Ah, 0CCh, 50h, 7Fh, 0E1h
                  db 70h, 1Ah, 0CDh, 71h, 7Bh, 0D6h, 49h, 7Dh, 0D5h, 83h
                  db 65h
```

[그림 7] RA Group 샘플에 내장된 Curve25519 공개키

```
C:\Users\vm\Desktop>keygen.exe
static const BYTE m_publ[] = { 0x58, 0xFB, 0xB8, 0xDD, 0x2B, 0x19, 0x00, 0xBA,
 0x1D, 0xA0, 0x79, 0x14, 0xCB, 0x67, 0xB2, 0xF4, 0x26, 0x5F, 0x52, 0xC3, 0x45,
 0xA9, 0x1C, 0x77, 0x55, 0x1E, 0x0F, 0xDC, 0xA0, 0x53, 0xAC, 0x20 };

static const BYTE m_priv[] = { 0x18, 0x57, 0x1F, 0xE8, 0xF9, 0xD3, 0x0D, 0xB8,
 0x7B, 0x8D, 0x78, 0x98, 0xFB, 0xE8, 0x89, 0x38, 0xA8, 0x06, 0xD0, 0x79, 0x6C,
 0x6C, 0x94, 0x90, 0x78, 0xE1, 0xFB, 0x2B, 0x2C, 0x15, 0x29, 0x77 };
```

[그림 8] 키젠을 통한 Curve25519 키 쌍 생성 예시

Babuk과 RA Group은 둘 다 Curve25519 암호 알고리즘을 활용하여 파일을 암호화한다.
Curve25519와 같은 타원곡선 암호는 RSA 암호보다 키 길이가 짧음에도 불구하고
그와 비슷하거나 더 높은 기밀성 수준을 제공하는 것으로 알려져 있다.
Babuk 소스코드에는 32바이트 크기의 공개키가 더미값으로 채워져 있지만,
[그림 7]의 RA Group 샘플은 일반적인 공개키가 채워져 있다.
유출된 파일에는 키젠이 동봉되어 있는데,
이를 사용하면 **[그림 8]**과 같이 무작위 Curve25519 키 쌍을 생성할 수 있었다.

```
else
{                                       // 파일의 크기가 10MiB를 초과할 경우,
                                        // 10MiB 블록마다 앞의 1MiB 데이터를 암호화한다.
  v38 = fileSize.QuadPart / 0xA00000;
  if ( fileSize.QuadPart / 0xA00000 > 0 )
  {
    do
    {
      ReadFile(FileW, v33, 0x100000u, &dwRead, 0i64);
      ECRYPT_process_bytes(v39, &ctx, v33, v33, dwRead);
      SetFilePointerEx(FileW, v36, 0i64, 0);
      WriteFile(FileW, v33, 0x100000u, &dwWrite, 0i64);
      v36.QuadPart += 0xA00000i64;
      SetFilePointerEx(FileW, v36, 0i64, 0);
      --v38;
    }
    while ( v38 );
  }
}
```

[그림 9] Babuk이 크기가 큰 파일을 암호화하는 방식

```
else
{                                       // 파일의 크기가 10MiB를 초과할 경우,
                                        // 2MiB 블록마다 앞의 1MiB 데이터를 암호화한다.
                                        // 이는 최대 10번까지만 반복한다.
  do
  {
    ReadFile(FileW, v34, 0x100000u, &dwRead, 0i64);
    ECRYPT_process_bytes(v38, v87, v34, v34, dwRead);
    SetFilePointerEx(FileW, v36, 0i64, 0);
    WriteFile(FileW, v34, 0x100000u, &dwWrite, 0i64);
    v36.QuadPart += 0x200000i64;
    SetFilePointerEx(FileW, v36, 0i64, 0);
    --v8;
  }
  while ( v8 );
}
```

[그림 10] RA Group이 크기가 큰 파일을 암호화하는 방식

RA Group은 크기가 큰 파일(10MiB 초과)에 대해 암호화를 할 때 다른 방식을 사용한다.
기존 Babuk 랜섬웨어는 10MiB마다 앞의 1MiB를 암호화시켜서 전체를 균일하게 암호화하였다.
그러나 RA Group은 2MiB마다 앞의 1MiB를 암호화시키는 방식으로 변경되었다.
후자의 방식은 파일의 시작부터 20MiB를 대상으로만 수행하므로
파일 크기가 110MiB 이상인 파일을 암호화할 때 RA Group이 더 좋은 성능을 낼 수 있다.


```
v2 = 2i64 * (lstrlenW(path) + 7);
do
  v3 = (WCHAR *)HeapAlloc(hHeap, 8u, v2 + 64);
while ( !v3 );
lstrcpyW(v3, path);
lstrcatW(v3, L".GAGUP");
result = MoveFileExW(path, v3, 9u);
```

[그림 11] 감염 파일 확장자 추가

감염 파일에 붙여지는 확장자는 “.GAGUP”으로 변경되었다.
그에 따라 랜섬웨어가 파일을 암호화할 때도 “.GAGUP” 확장자를 가진 파일은 암호화 대상에서 제외된다.

2.4. 차이점 4: 랜섬노트 생성

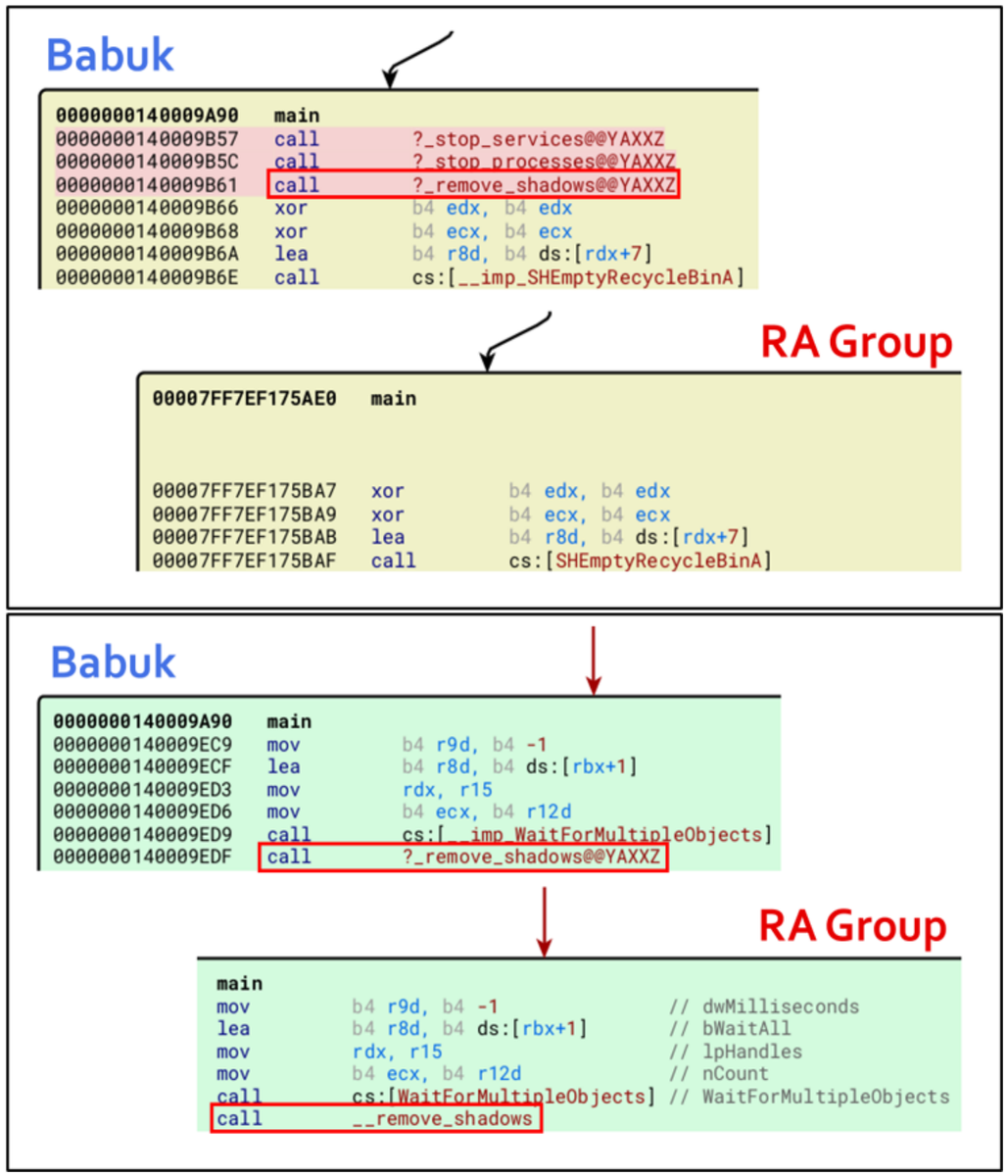
```
# RA Group
----
## Notification
Your data has been encrypted when you read this letter.
We have copied all data to our server.
But don't worry, your data will not be compromised or made public if you do what I want.

## What did we do?
We took your data and encrypted your servers, encrypted files can be decrypted.
We had saved your data properly, we will delete the saved data if you meet our requirements.
We took the following data:
```

[그림 12] 랜섬노트 본문

랜섬노트는 RA Group의 랜섬노트로 변경되었다.
본문에는 RA Group에서 운영하는 데이터 유출 사이트 주소와 qTox 메신저 연락처가 포함되어 있다.

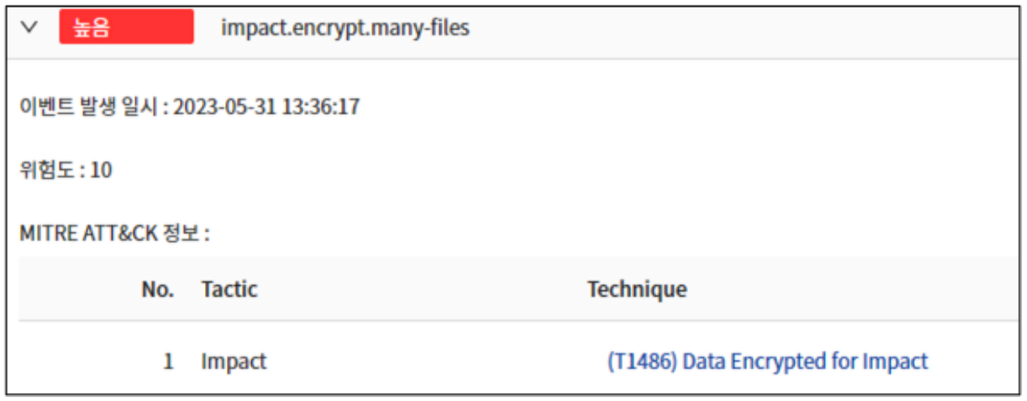
2.5. 차이점 5: 볼륨 섀도 카피본 삭제



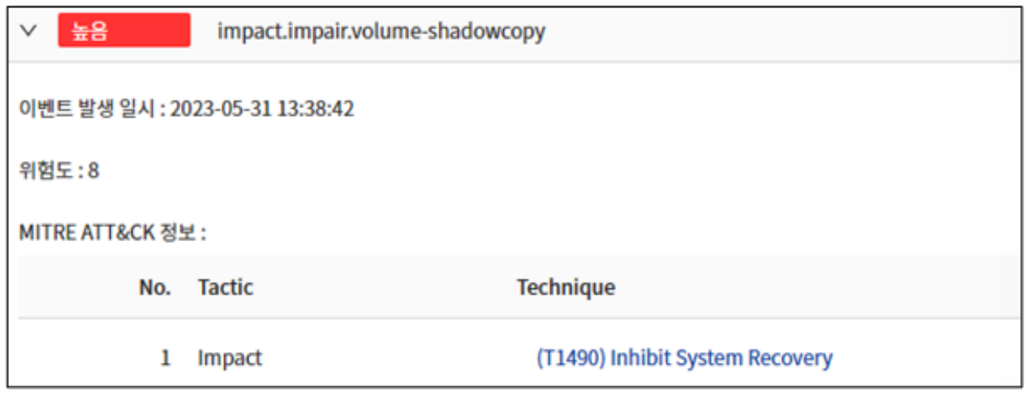
[그림 13] _remove_shadows 함수 호출 비교

볼륨 섀도 카피 서비스(Volume Shadow Copy Service)는
윈도우즈에서 기본적으로 제공하는 백업 기능이다.
기존 Babuk 랜섬웨어는 파일 암호화 전과 후에 각각 볼륨 섀도 카피본을 삭제하여
총 두 번 삭제하였다. RA Group은 파일 암호화 전에 볼륨 섀도 카피본을 삭제하는 코드는 제거하고,
파일 암호화 후에 볼륨 섀도 카피본을 삭제하는 코드만 남겨두었다.
vssadmin(볼륨 섀도 카피 서비스 보조 프로그램)을 사용해 삭제하는 방식에는 변함이 없다.

3. Privacy-i EDR 탐지 정보



[그림 14] Privacy-i EDR 파일 암호화 탐지



[그림 15] Privacy-i EDR 섀도 카피본 삭제 탐지

Privacy-i EDR은 행위 기반 탐지 엔진을 통해
RA Group 랜섬웨어의 파일 암호화와 볼륨 섀도 카피본 삭제 행위를 위와 같이 탐지하고 차단하였다.

4. 대응

1. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단한다
2. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션을 최신 형상으로 유지한다.
3. PC 취약점을 주기적으로 점검, 보완한다.
4. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지한다.
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단한다.
6. OS나 어플리케이션은 최신 형상을 유지한다.

5. 참고자료

5.1 국내 피해 현황

일시	기업명	피해 규모
2023.04.28	아이진(주)	이력서, 이메일, 정부과제 관련 자료, 코로나19 백신 연구 자료 등 1.4TB 크기의 데이터

5.2 국제 피해 현황

일시	기업명	피해 규모
2023.05.25	[무역] Eastern Media International Corporation	이메일, 재무 문서 등 500GB 크기의 데이터 (아직 일부 데이터만 공개됨)
2023.04.27	[유통] Bisco Industries	이메일, 직원 정보, 고객사 정보, 재무 문서 등 580GB 크기의 데이터
2023.04.27	[재무] Wealth Enhancement Group	직원 정보, 재무 문서 등 65GB 크기의 데이터
2023.04.27	[보험] Insurance Providers Group	직원 정보, 고객 정보, 재무 문서 등 441GB 크기의 데이터

5.3. 참고 자료

RA Group 랜섬웨어 다크웹
hxxp://pa32ymaeu62yo5th5mraikgw5fcvznnsiiwti42carjliarodltmqcqd.onion/

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오