JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 23, No. 6, pp. 1141-1149, Jun. 2022

Check for updates

Google Rapid Response 기반 랜섬웨어 공격 대응 방안

오 세 욱[1] · 손 태 식[2*]
[1]아주대학교 정보통신대학원 사이버보안학과 석사과정
[2*]아주대학교 소프트웨어융합대학 사이버보안학과 교수

Countermeasure of Ransomware Attacks based on Google Rapid Response

Se-Wook Oh[1] · Tae-Shik Shon[2*]

[1]Master's Course, Department of Cyber Security, Ajou University, Suwon World cup-ro 206, Korea
[2*]Professor, Department of Cyber Security, Ajou University, Suwon World cup-ro 206, Korea

[요 약]

인터넷 과 가상화폐의 발전으로 이를 악용하는 랜섬웨어 공격이 활발하게 진행되고 있다. 공격자는 개인, 기업, 공공기관에 상관없이 랜섬웨어 공격 후 거액의 금액을 요청하고 탈취한 피해자의 중요 정보들을 다크웹에서 판매 한다. 이러한 공격들을 방어하기 위한 여러 상용 솔루션들이 출시되고 있으나 적용 범위의 제한 또는 고가의 비용으로 인해 도입을 못하는 경우도 있다. 이러한 한계점을 극복하기 위해서는 무료로 배포 되면서 필요한 경우 코드 수정이 가능한 오픈소스 기반 보안 솔루션의 도입이 필요하다. 이번 연구는 오픈소스 기반 EDR 솔루션 중 GRR(Google Rapid Response)의 활용을 제안하고자 한다. 이에 DarkSide 랜섬웨어 코드와 공격 전술을 분석 후 해당 기법을 응용한 가상 공격 시 GRR의 어떠한 기능들을 활용하면 탐지가 가능한지 실험 하였다. 이후 실험 결과를 바탕으로 랜섬웨어 대응을 위한 최적의 활용 방법을 제시해 보고자 한다.

[Abstract]

With the development of the Internet and virtual currency, ransomware attacks that exploit it are actively proceeding. The attacker requests a large amount of money after the ransomware attack, regardless of individual, corporate, or public institution, and sells the stolen victim's important information on the dark web. Several commercial solutions are being released to defend against these attacks, but in some cases, they cannot be introduced due to limited application scope or high cost. In order to overcome this limitation, it is necessary to introduce an open source-based security solution that is distributed free of charge and can modify the code if necessary. This study intends to propose the use of GRR (Google Rapid Response) among open source-based EDR solutions. Therefore, after analyzing the DarkSide ransomware code and attack tactics, we tested which functions of GRR can be used to detect when a virtual attack using this technique is applied. Afterwards, based on the experimental results, we would like to suggest the optimal use method for responding to ransomware.

색인어 : 랜섬웨어, 오픈소스, 보안솔루션, EDR, GRR

Keyword : Ransomware, OpenSource, Security Solution, EDR, GRR

http://dx.doi.org/10.9728/dcs.2022.23.6.1141

Received 13 May 2022; **Revised** 08 June 2022
Accepted 14 June 2022

***Corresponding Author; Tae-Shik Shon**

Tel: +82- 031-219-3321
E-mail: tsshon@ajou.ac.kr

Ⅰ. 서 론

랜섬웨어는 금전적인 요구, 즉 몸값을 요구하는 악성 소프트웨어라는 의미로 몸값(Ransome)과 소프트웨어(Software)의 단어를 합성한 용어이다. 랜섬웨어는 공격자가 피해자에게 이메일 또는 정보제공을 위장한 악성코드를 실행시키도록 유도하여 피해자의 시스템을 침투 후 시스템 자체 또는 내부의 데이터를 이용하지 못하도록 암호화를 시킨다. 이후 피해자에게 복구에 필요한 대가 지급을 요청하여 금전적인 손해를 끼치도록 한다.

최초의 랜섬웨어는 지금으로부터 약 30년 전인 1989년 WHO가 주최한 AIDS 회담에서 Dr. Joseph. L Popp가 정상 파일을 위장한 파일 암호화용 악성파일을 회의 참석자들에게 배포한 것으로 알려져 있다[1]. 이후 랜섬웨어는 2000년 초반 인터넷의 대중화와 더불어 그 피해범위가 점점 더 확산되게 된다. 2010년 전후에는 가상화폐의 탄생으로 익명성을 갖춘 디지털 자금의 유통이 가능해지면서 2013년 비트코인을 요구하는 크립토락커 랜섬웨어가 국내에도 확산되어 개인 피해자들에게 금전적인 피해를 발생시켰다. 2015년에는 전 세계적으로 약 325백만 달러 피해가 발생하였는데 2021년에는 200억 달러로 피해가 확산 되었으며 2031년에는 3000억 달러에 이를 것으로 전망되고 있다[2].

랜섬웨어가 국내 대중에게 널리 알려지게 된 것은 2017년 워너크라이 랜섬웨어가 전 세계적인 피해를 일으킨 것이 계기가 된다. 해당 랜섬웨어는 Shadow Broker라는 해커 그룹이 공개한 美 국가안보국(NSA)에 의해 개발된 것으로 간주되는 EternelBlue의 공격 기법을 응용한 것이다. 해당 공격으로 약 23만대의 컴퓨터가 감염되었으며 전 세계적으로 여러 공공 기관 및 기업에 피해가 발생하였고 현재도 관련 변종이 활동 중이다[3].

2017년부터는 RaaS (Ransomware as a Service), 즉 랜섬웨어를 전문적으로 서비스해주는 조직이 나타나기 시작했다. RaaS는 랜섬웨어 제작자가 공격자에게 랜섬웨어 코드를 제공하고 코드제작 능력이 없는 공격자는 RaaS 제작자가 제공한 랜섬웨어를 이용하여 공격을 성공 후 금전적 이득을 나눠 갖는 구조이다[4]. 현재 상당수의 랜섬웨어 공격은 이러한 RaaS 방식의 구조를 토대로 이루어지고 있다.

최근에 랜섬웨어를 이용하는 공격자들은 감염 복구비용 탈취와 더불어 피해자 시스템 내 비공개된 주요 정보들(개인정보, 사내 주요 공문, 주요 설계도 등)을 유출 후 이를 추적이 어려운 다크넷에 광고를 올려 판매하거나 피해자에게 정보를 공개할 것이라 협박하여 금전을 탈취하는 전략도 함께 사용하고 있다. 이러한 공격을 수행하기 위하여 공격자는 특정 기업이나 공공기관을 목표로 지정 후 수개월에 걸쳐 지속적인 접근을 시도한다. 이후 내부 시스템 접근권한을 획득하면 정보 탈취를 성공한 후 랜섬웨어를 감염시키는 이중 공격을 시도하고 있다.

이렇게 진화하고 있는 랜섬웨어에 대처하기 위해서 여러 상용 솔루션이 개발되고 있는데 솔루션의 보안 대상에 대한 적용 범위 및 고가의 비용 지불 문제가 발생하여 도입이 지연되거나 중단되는 경우도 있다. 이에 무료로 제공하면서 코드 수정이 가능한 오픈소스 기반 보안 솔루션들이 대안으로 주목 받고 있다. 본 연구에서는 오픈소스 기반 보안 솔루션 중 EDR 기능을 지원하는 GRR(Google Rapid Response)을 활용하는 방법을 실험해 보았다.

본 논문의 구성은 2장에서 랜섬웨어의 특징 식별 및 탐지 방안에 대한 여러 연구 결과들과 EDR을 포함해 여러 오픈소스 들을 활용하여 악성코드 대처 방안에 대해 연구한 결과들을 살펴본다. 3장에서는 DarkSide 랜섬웨어에 대한 악성코드 분석 및 DarkSide의 공격으로 추정되는 콜로니얼 파이프라인 공격을 기준으로 공격 전술을 분석하였으며 GRR에 대한 정의 및 주요 기능에 대하여 분석하였다. 4장에서는 3장에서 분석된 DarkSide 랜섬웨어에 감염 되었을 때 GRR의 어떠한 기능을 이용하여 랜섬웨어 감염 여부를 확인 가능한지 실험해 보았다. 마지막으로 제 5장에서는 실험에 대한 결론과 향후 연구를 논의한다.

Ⅱ. 관련 연구

2010년 이후로 랜섬웨어 공격이 활발하게 진행됨에 따라 이를 탐지하거나 방어하기 위한 랜섬웨어 특징들을 분석하는 여러 연구들이 진행되었다.

이규빈 외 2인은 랜섬웨어 동적 분석을 위한 시그니처 추출 및 선정방법을 분석하였다[5]. 해당 연구에서는 악성코드 분석 시 정적 분석과 동적 분석을 진행하는데 최신 랜섬웨어 악성코드들의 패킹 기술이 고도화됨에 따라 정적분석의 한계가 있음을 지적하고 이에 대한 개선 방법으로 랜섬웨어 활동 모니터링 및 보다 정밀한 분석을 진행하기 위해 랜섬웨어 탐지에 적절한 시그니처를 선정하는 방법을 제안하였다.

최도현은 랜섬웨어 탐지를 위한 그래프 데이터베이스 설계 및 구현을 분석하였다[6]. 해당 연구에서는 다양한 경로를 통해 감염되는 랜섬웨어에 대하여 차단이 어려움 점을 인식하고 이를 개선하기 위하여 관계형 데이터베이스와 다른 그래프 데이터베이스 환경에서 랜섬웨어 패턴탐지가 가능하도록 그래픽 데이터베이스를 기반으로 랜섬웨어 악성행위를 모델링하고 랜섬웨어에 대한 새로운 다중복합 악성행위를 탐지하는 방법을 제안하였다.

이세훈 외 6인은 랜섬웨어 암호화 프로세스 및 복호화 방안을 분석하였다. 지능화된 랜섬웨어 5종(Gandcrab, Sodinokibi, Clop, Phobos, LooCipher)을 역 공학 하여 암호화 프로세스의 동작 방식을 밝히고 이를 기반으로 복구 방법에 대하여 제안하였다[7].

이진우 외 3인은 기존 랜섬웨어 탐지연구는 프로세스의 특

정 행위를 감시하거나 시그니처 데이터베이스를 활용하여 탐지하기 때문에 신종 랜섬웨어가 실행되는 경우 탐지하고 차단이 어려울 것으로 판단하였다. 이에 해당 연구에서는 파일시스템에 접근하고 동작하는 방식을 분석하여 랜섬웨어가 파일을 감염을 시키는 경로정보를 분석 후 미끼 파일을 배치하여 기존 방식보다 신속한 탐지가 가능한 방법을 제안하였다[8].

악성코드를 방어하는데 있어 상용 보안 솔루션이 아닌 오픈소스 기반 보안 솔루션을 이용한 탐지 방법에 대해서도 다양한 연구가 진행되었다.

이수진 외 5인은 오픈소스 엔드포인트 탐지를 사용하여 네트워크 및 시스템 수준에서 체계적인 랜섬웨어 탐지가 가능한 프레임워크 환경을 구축하고 연구를 진행하였다[9]. RAASNet 오픈소스 랜섬웨어를 실행 하였을때 오픈소스 엔드포인트 기반 EDR 3종을 선발하여 랜섬웨어 실행 시점에 탐지가 되는지를 검증하였다.

석진욱 외 2인은 오픈소스 IDS, IPS로써 무료 배포중인 Suricata를 적용한 Windows7과 Ubuntu의 성능을 비교 연구하였고 각 운영체제에서 CPU 사용률을 비교해 본 결과 Ubuntu에서는 Suritaca 동작 시 멀티코어 환경에서 균일한 사용률을 보여 Windows7보다 더 우수한 결과를 가져옴을 확인하였다[10].

윤다예 외 6인은 오픈소스 기반의 네트워크 통합보안시스템을 연구를 위하여 임베디드 오픈소스 보안 OS인 OpenWRT를 이용하여 보안 기능이 구현된 펌웨어를 제작 배포, 테스트 검증 과정을 진행하였다[11]. 검증 결과 문제 발생률 30%미만의 안전한 시스템 요건을 충족하였으며, 실제 상용 네트워크 환경에 부합하는 사양으로 테스트를 수행하여 사용자가 원하는 수준의 성능을 보여준 것을 확인하였다.

김희은 외 4인은 오픈소스 기반 APT 공격 예방 Chrome extension 개발을 연구하였다[12]. 기존 CDR은 파일의 잠재적인 요소를 원천 제거 후 안전한 파일로 재조합하여 악성코드를 차단해 주나 일부 미 지원되는 파일(HWP)들이 있기에 DangerZone 오픈소스를 활용하여 HWP을 지원하고 Chrome extension개발을 통해 상용메일 URL의 검사도 가능한 개발 프로젝트를 진행 후 성능을 입증하였다.

이와 같이 여러 연구에서 랜섬웨어의 특징들을 다양한 관점으로 분석 후 탐지율을 높이기 위한 방안들이 제시되고 있으며 오픈소스를 활용하거나 추가 개발을 통하여 악성행위를 탐지하는 여러 방안들도 제시되고 있다.

Ⅲ. 본 론

본 논문에서는 2021년 전 세계적으로 큰 이슈를 남겼던 주요 랜섬웨어 중 DarkSide 랜섬웨어 코드분석과 공격전술을 분석해보고 해당 공격을 탐지 및 방어하기 위한 오픈소스 EDR 중 GRR을 활용하는 방법을 제안한다.

3-1 DarkSide 랜섬웨어 코드 분석

러시아와 동유럽에 기반을 둔 공격조직인 DarkSide는 공격기법이 정교하고 기술적인 능력이 뛰어나며 고가의 보상금을 요구하는 것으로 악명 높은 그룹이다. 2021년 5월 미국 대형 송유관 운영사인 콜로니얼 파이프라인을 공격하여 미 남동부 일대 석유 공급에 큰 차질을 일으킨 바가 있다. 당시 공격자는 송유관 모니터링 시스템에 접근 비밀번호를 획득 후 내부 시스템 침투에 성공하여 공격을 진행한 것으로 추정된다. 이후 회사는 공격자가 요청한 75 비트코인(당시 $4.4 백만)을 지불 후에야 시스템을 복원할 수 있었다[13].

코드 분석에 이용한 DarkSide 랜섬웨어 파일의 기본 정보는 표 1과 같다. 해당 랜섬웨어 코드는 콜로니얼 파이프라인 공격 이전에 생성된 코드로 콜로니얼 파이프라인 공격에 사용되었는지는 확인되지 않았으나 공격에 사용된 파일과 유사 구조였을 것으로 추정된다. 해당 코드는 코드 분석이 어렵도록 공격자가 자체 생성한 패킹 기법이 적용되어 있다.

표 1. DarkSide 랜섬웨어 파일 속성 정보
Table. 1. DarkSide Ransomware File Attribute Information

Category	Description
File Name	idfoodsf.exe
Hash Info (SHA-256)	0839AABE5FD63B16844A27B3C586C02A044D 119010A1A40EE4035501C34EAE0D
Create Date	20201223 17:01:07 UTC
Pack	Unknown

동적 분석 툴을 이용하여 패킹된 부분을 해제 후 정적 분석 툴과 함께 해당 코드를 분석한 결과는 다음과 같다.

가. 라이브러리 불러오기

악성코드는 그림 1과 같이 최초 실행 시 랜섬웨어 동작에 필요한 시스템 라이브러리를 호출한다. 난독화된 문자열이 하드코딩 되어 있으며 이를 메모리에 불러 온 후 자체 복호화 함수로 변환하면 커널 라이브러리명이 생성된다. 이후 생성된 라이브러리 명을 인자 값으로 하여 LoadLibray API를 호출하면 Kernel32를 포함한 총 15개의 시스템 라이브러리가 등록된다.

```
ConvertString_4016D5((int)v1, v2);              // kernel32
v3 = LoadLibraryA(v1);
Clean_4013DA(v1, *((_DWORD *)v1 - 1));
v4 = &v1[*((_DWORD *)v1 - 1)];
LoadAPI_401AC3(v3, (FARPROC *)&wcsicmp_410CD6, v4);
v5 = *(_DWORD *)v4;
v4 += 4;
ConvertString_4016D5((int)v4, v5);              // advapi32
v6 = LoadLibraryA(v4);
Clean_4013DA(v4, *((_DWORD *)v4 - 1));
v7 = &v4[*((_DWORD *)v4 - 1)];
LoadAPI_401AC3(v6, (FARPROC *)&wcsicmp_410CD6, v7);
v8 = *(_DWORD *)v7;
v7 += 4;
ConvertString_4016D5((int)v7, v8);              // shell32
```

그림 1. 시스템 라이브러리 호출
Fig. 1. Call System Library

난독화 된 문자열을 복호화 하는 방법은 그림 2와 같이 전체 문자열을 255 byte단위로 구분 후 동일한 크기의 복호화 키와 XOR 연산을 통해서 복호화를 진행하는 함수를 이용한다. 해당 함수는 악성코드에 있는 여러 난독화 된 문자열들을 해독하는데도 동일하게 사용된다.

```
v2 = a1_String;
v3 = a2_length / 255;
v4 = a2_length % 255;
if ( a2_length / 255 )
{
  v5 = a2_length / 255;                         // Share
  do
  {
    LOBYTE(v3) = XOR_Decoder_4017AA(v2, 255);
    v2 += 255;
    --v5;
  }
  while ( v5 );
}
if ( v4 )                                       // Reminder
  LOBYTE(v3) = XOR_Decoder_4017AA(v2, v4);
```

그림 2. 문자열 복호화 함수
Fig. 2. String decryption function

나. 실행 권한 확인 후 변경(관리자 권한 획득)

악성코드는 그림 3과 같이 IsUserAnAdmin 라는 API를 이용하여 현재 계정이 관리자권한을 가지고 있는지 확인하며 이후 AdjustTokenPrivileges API 등을 이용하여 관리자 권한으로 변경시킨다.

```
GetTokenInformation_410E52(v6, 3, &v5, 4, &v4);
v1 = RtlAllocateHeap_410D56(dword_410A9E, 8, v4);
v5 = v1;
result = GetTokenInformation_410E52(v6, 3, v1, v4, &v4);
if ( result )
{
  v2 = v5 + 4;
  v3 = *(_DWORD *)v5;
  do
  {
    if ( !*(_DWORD *)(v2 + 8) )
      *(_DWORD *)(v2 + 8) = 2;
    v2 += 12;
    --v3;
  }
  while ( v3 );
  result = AdjustTokenPrivileges_410E5A(v6, 0, v5, 0, 0, 0);
}
```

그림 3. 권한 변경 확인
Fig. 3. Confirm permission change

다. 시스템 고유 식별자(ID) 확인

악성코드는 그림 4와 같이 시스템의 사용자 고유 식별 정보를 이용하기 위하여 Cryptography 레지스트리에서 MachineGuid의 데이터를 읽는다. 이후 CRC32 해쉬를 이용하여 생성된 값을 랜섬웨어의 확장자로 사용한다.

```
v2 = ConverString_Extension_401AEC(&unk_40B80E);// SOFTWARE\Microsoft\Cryptography
if ( !RegOpenKeyExW_410E82(0x80000002, v2, 0, 257, &v15) )
{
  v14 = 1;
  v13 = 128;
  v3 = ConverString_Extension_401AEC(&unk_40B852);// MachineGuid
  if ( !RegQueryValueExW_410E9A(v15, v3, 0, &v14, &v11, &v13, v10) )
  {
    v4 = WideCharToMultiByte_410E1E(0, 0, &v11, -1, &v12, 64, 0, 0);// 2aa07ace-109d-42
    v5 = CRC32_401E10((int)&v12, v4, 0);
    v6 = CRC32_401E10((int)v5, 16, 1);
    v7 = CRC32_401E10((int)v6, 16, 1);
    v8 = CRC32_401E10((int)v7, 16, 1);          // CRC Hash
    *a2 = 46;
    sub_40151D(v8, 4, a2 + 1);                  // Set extension(13e99088) by using HW ID
```

그림 4. 시스템 ID 변환과정
Fig. 4. System ID conversion process

라. 파일 암호화

악성코드는 그림 5와 같이 암호화 단계 진입 시 시스템 언어 정보를 비교하여 특정 언어(Russian Speaking 등 14개 지역)를 사용하는 시스템의 경우 암호화를 시작하지 않는다. 이러한 특징을 통해 Darkside는 러시아어를 사용하는 국가들과 관련이 있는 조직으로 추정된다.

```
if ( F_Debug_41092C )                           // System Language Check
{
  ConvertString_4016D5((int)&unk_40B29E, a2_length);
  sub_403E63(F_Debug_41092C, (int)&unk_40B20A, (int)&unk_40B29E, 0, 0);
  Clean_4013DA(&unk_40B29E, a2_length);
}
result = Get_LangID_404819();                   // Check System Language
if ( result )
{
  if ( F_Debug_41092C )                         // This is a Russian-Speaking
  {
    ConvertString_4016D5((int)&unk_40B2CE, dword_40B2CA);
    sub_403E63(F_Debug_41092C, (int)&unk_40B20A, (int)&unk_40B2CE, 0, 0);
    result = Clean_4013DA(&unk_40B2CE, dword_40B2CA);
  }
```

그림 5. 시스템 언어 확인
Fig. 5. Check System Language

악성코드는 그림 6과 같이 연결되어 있는 디스크 드라이버 정보를 확인하며, 안티 디버깅 서비스 및 프로세스를 종료 한 후 시스템 내 특정 확장자들을 제외한 파일들에 대한 암호화를 진행한다.

```
v0 = GetLogicalDriveStringsW_410DC2(128, &v5);// Get DriveInfo
if ( v0 )
{
  v1 = &v5;
  v2 = v0 >> 2;
  do
  {
    v3 = GetDriveTypeW_410DC6(v1);              // Check DriveType
    if ( v3 == 3 || v3 == 2 || v3 == 4 )        // 3=Fixed, 2=Removable, 4=Network
    {
      v6 = '\\0\\';
      v7 = '\\0?';
      wcscpy_410CDE(&v8, v1);
      Ransomware_CoreProcess_406B07(v4, (int)&v6);
    }
    v1 += 2;
    --v2;
  }
  while ( v2 );
}
```

그림 6. 드라이버 확인 및 파일 암호화
Fig. 6. Check driver and encrypt files

암호화 까지 완료한 악성코드는 별도 이미지 파일을 만든 후 Wallpaper 레지스트리의 배경화면 경로를 새로 만든 이미지의 경로로 변경함으로써 그림 7과 같이 바탕화면에 랜섬웨어에 감염된 상황임을 피해자에게 보여준다.

그림 7. 랜섬웨어에 감염된 PC의 바탕화면
Fig. 7. PC desktop infected with ransomware

또한, 그림 8과 같이 각 폴더별 랜섬노트를 함께 생성하는데 랜섬노트에는 특정 .onion 주소가 기재되어 있으며 해당 주소로 접속 시 가상화폐 지갑주소로 복호화를 위한 대가 지급을 요구한다.

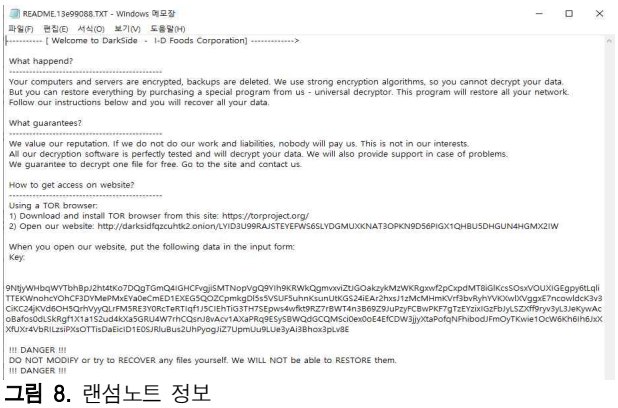

그림 8. 랜섬노트 정보
Fig. 8. Ransom Note Information

3-2 DarkSide 랜섬웨어 공격 전술 분석

DarkSide 랜섬웨어 공격 조직의 콜로니얼 파이프라인 공격에 대하여 언론 및 기관에서 공개한 정보를 토대로 최초 정찰단계부터 정보탈취 및 랜섬웨어 감염인 목적수행 까지 7단계의 공격전술로 분류하여 분석하였다.

가. 정찰

공격자는 의도적인 목적으로 목표에 접근한 것으로 추정된다. 내부 시스템에 접근을 위한 정찰단계로 회사 웹사이트에 등록되어 있는 정보들을 수집한다. 예를 들어 공개된 페이지에서 제어시스템 장비 모델명과 상세 정보가 표시된 이미지 파일 등을 다운로드 하여 공격 대상의 정보를 수집 후 분석한다.

나. 스피어피싱 메일

공격자는 내부 직원들에게 스피어피싱 메일을 발송하며 회사 원격서버에 있는 파일들을 검색하기 위한 악성링크를 포함시킨다. 이후 정상메일로 오판한 피해자가 악성링크를 클릭하여 서버에게 검색 요청을 할 때 사용자 고유정보(해쉬값)를 함께 전달하는데 공격조직은 이 데이터를 가로챈 후 암호 해독 기술을 이용, 피해자 암호를 획득함으로써 SSO 인증에 접근할 수 있는 권한을 확보한다.

다. 워터링 홀

공격자는 또 다른 방법으로 워터링 홀을 사용한다. 공격자는 회사와 관련 있는 공정제어 또는 인프라 정보가 있는 웹사이트를 변조하며 주요 악성행위는 스피어피싱 이메일에 사용된 기법과 같이 서버 접속을 유도 후 SSO 인증에 접근 할 수 있는 암호를 획득한다.

라. 계정 탈취

공격자는 피해자의 계정 정보 탈취를 위하여 다른 스피어피싱 이메일을 사용한다. 계약 문서나 이력서와 같은 일반적인 문서로 위장된 악성파일을 이메일로 배포하며 피해자가 해당 문서 또는 이메일에 기재되어 있는 링크를 누르면 계정과 암호를 묻는 피싱사이트로 접속하게 된다.

마. 공격거점 생성

이메일 내에 있는 악성 링크는 단축 URL(bit.xx 등)를 통해 다른 사이트로 리다이렉트 된 후 공격자가 만들어 놓은 명령제어 서버에 접속하게 된다. 또한, 악성문서를 실행하는 경우도 악성문서 내 포함되어 있는 스크립트와 악성파일들에 의해 명령제어 서버에 접속하게 된다. 명령제어 서버는 회사 도메인에 인증을 유도하거나 사용자 이름과 암호를 확보하도록 설정되어 있다.

바. 악성코드 설치 및 명령제어

공격자는 피해자로부터 얻은 정보를 이용하여 회사 네트워크에 접속 후 지속적인 접속을 위하여 로컬 관리자 계정을 생성하고 악성코드를 설치한다. 이후 시스템 내 코드 탐색 및 원격접속용 계정, 가짜 관리자 계정, Microsoft Exchange 서버 관리자 계정, 로그 및 접근 정보 삭제 계정 등 개별적인 목적의 계정들을 생성한다.

이외에도 공격자가 피해자 시스템에서 노출 없이 활동하기 위하여 자동 로그아웃 기능 설정, 네트워크 탐지 회피를 위한 VPN 클라이언트 프로그램 사용, 공개용 SW 및 파이썬 등을 사용하며 원격서버에서 추가로 필요한 공격도구를 다운로드 하고 외부에서 내부 네트워크 접근을 위한 웹셸을 설치한다.

사. 목적수행

공격자는 VPN, RDP, OWA와 같은 원격 접속 서비스 및 인프라들을 활용한 것으로 확인된다. 이에 자격증명을 획득한 공격자는 RDP를 통해 피해자 도메인의 컨트롤러에 접근하며 호스트 정보, 사용자 정보, 환경 정보를 수집한 후 압축을 한다.

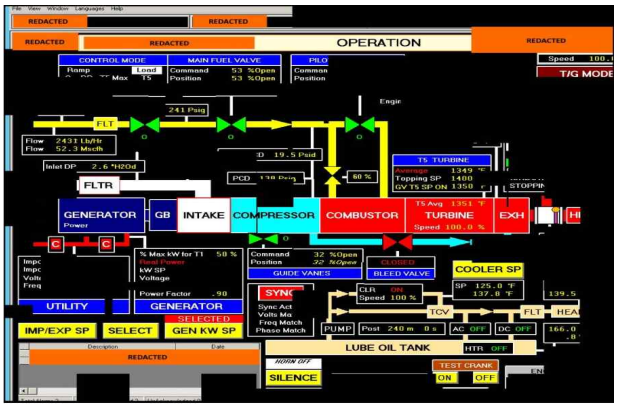

그림 9. 공격자에게 노출된 ICS 정보
Fig. 9. ICS information exposed to attackers

또한 공격자는 악성파일을 이용하여 시스템 화면을 캡처 후 특정 디렉토리에 JPEG 형식으로 저장 후 파일들을 압축하고 회사 네트워크에 연결된 워크스테이션과 서버에 접근하여 그림 9와 같이 ICS와 SCADA 시스템과 관련된 파일들에 접근 후 내용을 복사한다. 이후 공격자는 수집된 정보 중 일부를 RClone 또는 Putty와 같은 무료 접속 프로그램을 이용하여 탈취 하고 시스템 내부에 랜섬웨어를 실행시켜 시스템의 동작을 멈추게 하고 거액의 금전을 요구한다.

3-3 GRR(Google Rapid Response) 구성

APT 공격 기반의 랜섬웨어는 단일 방어 도구로는 방어가 어렵다. 기본적으로 공격대사의 환경 정보를 사전에 확인 후 시스템 취약점 정보를 활용하여 다양한 변종의 형태로 공격을 지속하게 된다. 이러한 공격에 가장 효율적인 방법으로 각광받고 있는 것은 EDR(Endpoint Detection and Response)라 하겠다. EDR을 활용하면 호스트 시스템의 정보를 파악 후 공격의 징후를 파악할 수 있고 시계열적인 데이터 소스의 변화를 확인함으로써 공격의 시작과 진행 시점의 파악이 가능하다. 그러나 EDR을 적용함에 있어 규모가 크지 않은 시스템 관리자 입장에서는 시중에 나와 있는 고가의 EDR을 적용하는 것은 제한이 있다. 이에 오픈소스 기반의 EDR을 활용한 방어기법을 적용하여 최신 랜섬웨어의 탐지가 가능한지를 확인하고자 하며 그 중 대표적으로 GRR을 활용하여 분석을 진행해 보고자 한다.

GRR은 구글에서 개발한 원격 라이브 포렌식에 중점을 둔 침해사고 대응 오픈소스 프레임 워크로서 파이썬 기반의 서버와 에이전트로 구성되어 있으며 '22년 4월 기준 v3.4.5.1 버전까지 릴리즈 되어 있다.

GRR 프레임워크는 서버와 클라이언트 프로그램으로 구성되어 있으며 서버 프로그램의 경우 그림 10과 같이 다수의 클라이언트에 대한 통합관리가 가능한 GUI 화면 및 기능을 제공하며 대규모 시스템에 적용하여도 무리가 없는 확장성을 제공한다. 이에 다수의 디지털 포렌식 아티팩트들을 쉽고 빠르게 수집 가능하며 효율적인 일정 관리를 위한 비동기적 설계를 갖추고 있다.

클라이언트 프로그램의 경우 리눅스, Apple Mac, 윈도우 등 크로스플랫폼을 지원한다. 각 OS 환경에서 메모리 분석을 할 수 있는 Rekall 프레임 워크를 사용하여, 원격지에서 활성화된 메모리 분석이 가능하며 각 아티팩트를 효과적으로 검색하고 다운로드 할 수 있다. 또한 필요에 따라 데이터 송수신 시 암호화를 적용하여 기밀성도 제공한다.

GRR 클라이언트 프로그램은 백그라운드 프로세스로 동작하며 클라이언트 프로그램 실행 후 서버 웹 화면에서 클라이언트 IP를 검색 시 그림 11과 같이 클라이언트 PC에 대한 정보가 표시된다.

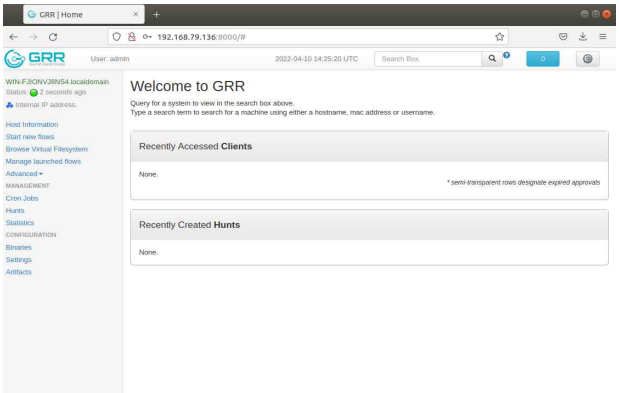

그림 10. GRR 서버 GUI 화면
Fig. 10. GRR Server GUI screen

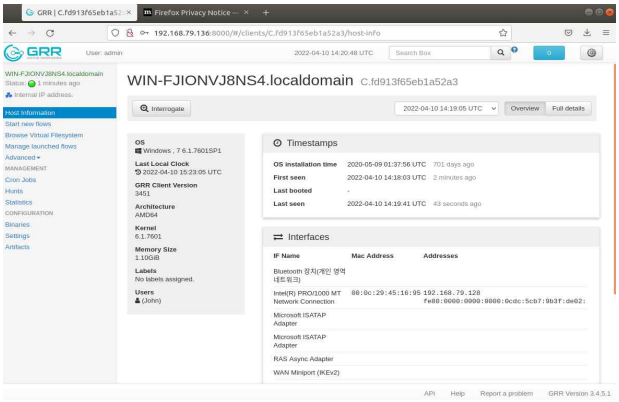

그림 11. GRR 클라이언트 정보 화면
Fig. 11. GRR Client Information Screen

서버에서는 단일 클라이언트에 대해서는 Flow 또는 다수의 클라이언트들에 대해서는 Hunts 기능을 이용하면 디바이스의 정보 확인이 가능하다. Flow는 클라이언트로부터 특정 리소스의 정보를 확인하고자 할 때 해당 경로 정보 또는 문자열(명령어) 정보를 입력 후 클라이언트로 요청하게 되며 클라이언트는 요청한 사항에 대한 검색 결과를 서버로 회신하게 된다. Flow 생성 및 요청 이후 관리자 테이블을 통하여 현재 상태, 경로, Flow 명칭, 날짜, 마지막 활성화된 시간 확인이 가능하며 클라이언트 응답이 오면 알림을 통하여 결과 값을 회신 받을 수 있다.

Ⅳ. 실험 및 분석

4-1 실험 준비

랜섬웨어 공격을 실험하기 위하여 가상환경(VMWare 15.1.0) 상에서 GRR 서버와 클라이언트 프로그램은 최신 버전(v3.4.5.1.)을 설치하였다. 시험에 사용된 서버와 클라이언트의 시스템 및 운영환경 정보는 표 2.와 같다.

표 2. 실험 환경 정보
Table. 2. Experimental environment information

Server	Client
VMWare : 15.1.0 OS : Ubuntu 18.04 Memory : 2GB Processors : 2 HDD : 20GB MySQL : 5.7.37 fleetspeak : No GRR_server_3.4.5.1.deb IP : 192.168.79.132 Port : 8000	VMWare : 15.1.0 OS : Windows7 SP1 Memory : 2GB Processors : 2 HDD : 40GB GRR_3.4.5.1_amd64.exe

이후 DarkSide 조직에서 사용한 공격전술 중 GRR에서 탐지 가능한 부분은 어떤 것들이 있는지 유사 공격 테스트를 진행해 보았으며 진행 결과는 다음과 같다.

4-2 실험 방법 및 결과

DarkSide 조직이 보여준 APT 공격과 병행한 랜섬웨어 공격 전술은 앞서 언급한데로 가. 정찰, 나. 스피어피싱, 다. 워터링홀, 라. 계정탈취, 마. 공격거점 생성, 바. 악성코드 설치 및 명령제어, 사. 목적 수행 단계로 이루어지게 된다.

가.~ 다. 의 미끼를 통한 최초 침투 과정을 진행 후 라. ~ 바. 의 과정을 거치게 되면 공격자는 계정정보를 탈취하는 과정이나 이후 과정에서 해당 시스템 정보를 스캔하기 위한 백도어 프로그램 실행을 하게 된다. 이러한 백도어 프로그램의 경우 외부에서 내부로 접근 과정이 필요하기에 네트워크 정보를 모니터링 함으로써 악성행위를 탐지할 수 있다. 그림12와 같이 GRR의 Flow에서 Network → Netstat 기능으로 현재 오픈되어 있는 포트 정보 및 연결되어 있는 IP 정보 확인이 가능하다. 실제 외부에서 클라이언트 영역으로 PSExec와 같은 원격 접속용 프로그램으로 접속한 상태에서 Flow의 Network → Netstat 기능을 호출한 결과 백도어 프로그램과 연결된 외부 네트워크 접속 확인이 가능하였다.

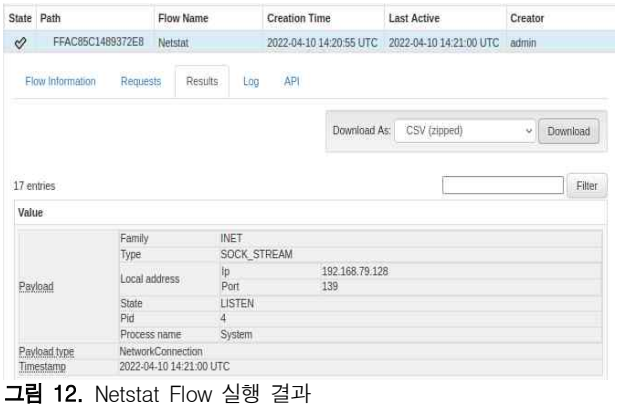

그림 12. Netstat Flow 실행 결과
Fig. 12. Netstat Flow Result

사. 목적수행 단계 즉, 랜섬웨어 코드 설치 및 실행 단계의 경우로 랜섬웨어 악성코드 분석을 토대로 다음 두 가지 측면에서 변화를 관찰할 수 있다. 첫 번째로는 그림 13과 같이 DarkSide 랜섬웨어의 특징 중 하나인 배경화면을 랜섬노트로 변경하는 과정으로 레지스트리의 Control Panel 내부에 Wallpaper 의 경로가 변화된 것으로 확인이 가능하다.

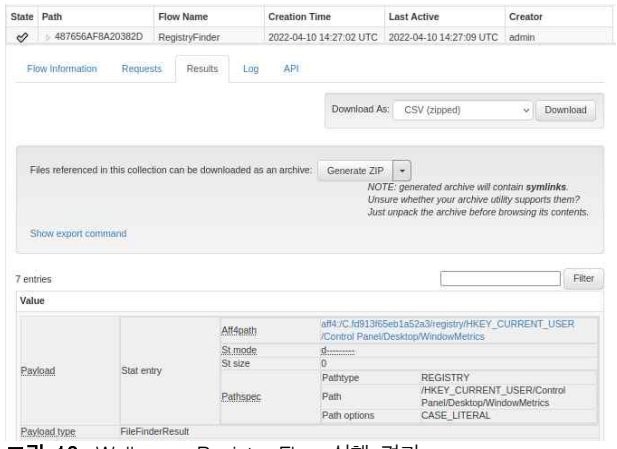

그림 13. Wallpaper Registry Flow 실행 결과
Fig. 13. Wallpaper Registry Flow Result

두 번째로는 그림 14, 그림 15와 같이 랜섬웨어로 인한 파일 변경 과정을 GRR의 FileFinder를 이용하면 파일의 MAC Time 정보 변경 및 파일 확장자명이 변경되는 것을 식별할 수 있다. MAC Time 정보의 경우 랜섬웨어에 의한 암호화 및 확장자 명 변경과정에서 시간 정보가 변경되며 실제 실험에서도 랜섬웨어에 감염된 이후 테스트 샘플의 Mtime 정보가 변경되어 있는 것을 확인하였다. 여기에 추가적으로 랜섬웨어 감염 과정에서 각 폴더별로 README_(XXXXXXXX).txt 랜섬노트 파일이 함께 생성된다. 이에 해당 폴더 내 전체 파일에 대하여 FileFinder로 검색해 보면 랜섬노트의 생성유무도 확인이 가능하다.

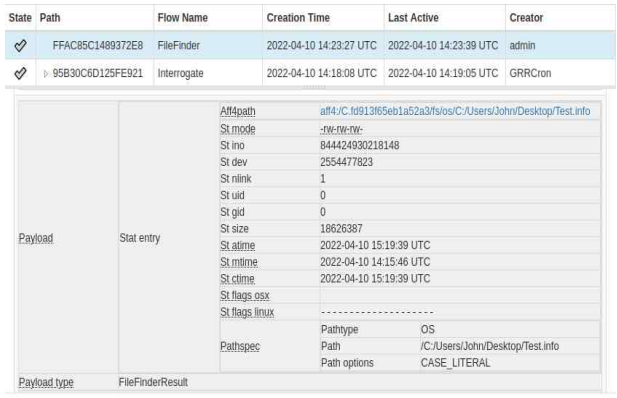

그림 14. FileFinder Flow를 이용한 파일 속성 정보 확인
Fig. 14. Checking file attribute information using FileFinder Flow

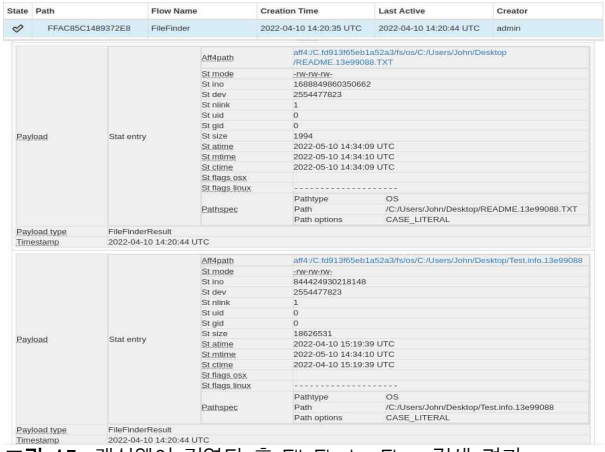

그림 15. 랜섬웨어 감염된 후 FileFinder Flow 검색 결과
Fig. 15. FileFinder Flow Result after Ransomware infection

위와 같이 DarkSide 랜섬웨어는 GRR의 Flow 나 Hunt 기능을 이용하여 네트워크, 레지스트리, 파일속성 정보들을 지속적으로 확인하면 초기 공격자의 행위 및 랜섬웨어 감염의 징후 탐지가 가능함을 확인하였다.

V. 결 론

이번 연구는 최근 활발하게 활동 중인 여러 랜섬웨어 조직 중 美 콜로니얼 파이프라인을 공격한 DarkSide 공격 조직의 공격기법을 확인하였고 오픈소스 EDR 중 하나인 GRR에서 유사 공격 발생 시 탐지가 가능한지 확인하였다. 이러한 탐지를 위하여 Darkside 랜섬웨어 실제 공격코드를 분석하여 코드 내 특징들을 식별하였고 외부 공개 정보들을 토대로 그들이 사용하는 공격전술은 어떠한 것이 있는지 분석해 보았으며 이를 토대로 GRR 모니터링 과정에서 어떠한 데이터를 중점적으로 관찰하고 분석을 해야 하는지 실험해 보았다.

공격기법을 확인한 결과 DarkSide 랜섬웨어 공격자들은 다양한 도구와 우회 방법들을 사용하고 있으나 시스템 침입 후 파일 탈취와 암호화 과정은 기존에 알려져 있는 다른 랜섬웨어 공격기법과 유사한 것으로 확인된다. 이에 따라 GRR의 Flow 기능을 이용하여 클라이언트의 네트워크, 레지스트리, 파일 속성 값의 변화 들을 주기적으로 관찰하게 되면 최신 랜섬웨어 공격에 있어서도 효율적인 탐지가 가능한 것을 확인하였다. 이에 해당 특징들을 이용하여 파이썬과 같은 프로그램 언어를 이용해 GRR과 연동 가능한 자동 탐지 툴을 자체 개발하면 상용 EDR과 대등한 기능 구현이 가능할 것으로 예상된다. 이러한 응용방법은 고가의 비용이나 대상 범위의 제한으로 상용 EDR 도입이 제한되었던 기업과 보안 담당자들에게 도움을 줄 수 있을 것으로 기대한다.

향후 연구 계획은 이번 공격 전술 분석 대상이었던 DarkSide 랜섬웨어 이외에도 다른 주요 랜섬웨어 조직들에 대한 공격 전술 분석하고 이를 탐지하는 방법을 찾아봄으로써 GRR의 활용 범위를 넓히고자 한다. 또한, GRR 이외에도 다른 오픈소스 EDR 솔루션들에 대한 비교 테스트를 진행하여 랜섬웨어에 가장 효율적인 EDR솔루션을 제시해 보고자 한다.

참고문헌

[1] WIKIPEDIA website, https://en.wikipedia.org/wiki/Ransomware

[2] H.Y.Kim, S.E.Jang, B.H.Choi, Ransomware Special Report, KISA, p2-4, Sep, 2021

[3] TrendMicro, Malware Using Exploits from Shadow Brokers Leak Reportedly in the Wild https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats

[4] CrowdStrike, RANSOMWARE AS A SERVICE (RAAS) EXPLAINED https://www.crowdstrike.com/cybersecurity-101/ransomware /ransomware-as-a-service-raas/

[5] Gyu Bin Lee, Jeong Yun Oak, Eul Gyu Im, “Method of Signature Extraction and Selection for Ransomware Dynamic Analysis”, KIISE Transactions on Computing Practices 24(2), pp 99-104, Feb. 2018 https://doi.org/10.5626/KTCP.2018.24.2.99

[6] Do-Hyeon Choi, “Graph Database Design and Implementation for Ransomware Detection”, Journal of Convergence for Information Technology Vol.11. No.6, pp.24-32, June. 2021 https://doi.org/10.22156/CS4SMB.2021.11.06.024

[7] Sehoon Lee, Byungchul Youn, Soram Kim, Giyoon Kim, Yeongju Lee, Daeun Kim, Haeryong Park, Jongsung Kim, “A Study on Encryption Process and Decryption of Ransomware in 2019”, Journal of The Korea Institute of Information Security & Cryptology VOL.29, NO.6, pp 1,339-1,350, Dec. 2019 https://doi.org/10.13089/JKIISC.2019.29.6.1339

[8] Jinwoo Lee, Yongmin Kim, Jeonghwan Lee, Jiman Hon, “An Efficient Decoy File Placement Method for Detecting Ransomware”, Journal of The Smart Media VOL.8, NO.1, pp. 27-34, Feb. 2019

[9] Sun-Jin Lee, Hye-Yeon Shim, Yu-Rim Lee, Tae-Rim Park, So-Hyun Park, Il-Gu Lee, “Study on Systematic Ransomware Detection Techniques”, International Conference on Advanced Communications Technology(ICACT), Feb. 2021

[10] Seok Jinug･Kim Jimyung･Choi Moonseok, “The Comparative Study on Performance Analysis of Windows 7 and Ubuntu Applying Open Source IDS/IPS Suricata”,

Journal of Digital Industry Information Society Vol. 13 No. 4, pp. 141-151, Dec. 2017
http://dx.doi.org/10.17662/ksdim.2017.13.4.141

[11] Yoon Da Yea, Lee Jae Hwan, Lee Gi Su, Lee Yeon Bum, Jeong Sung Min, Cho Sung Jae, Han Cheol Gyu, “Open Source based Network United Security System”, Proceedings of the 2015 Winter Academic Conference, pp. 1,555-1,557, Dec. 2015

[12] Heeeun Kim, Taeshik Shon, Duwon Kim, Gwangseok Han, JiHoon Seong, “Development of an open source-based APT attack prevention Chrome extension”, JOURNAL OF PLATFORM TECHNOLOGY VOL. 9, NO. 3, pp. 3-17, Sep. 2021

[13] WIKIPEDIA website, https://en.wikipedia.org/wiki/Colonial _Pipeline_ ransomware_attack

오세욱(Se-Wook Oh)

2020년～현　재 : 아주대학교 정보통신대학원 사이버보안학과 석사과정

※관심분야 : 사이버보안, 악성코드, 랜섬웨어 등

손태식(Tae-Shik Shon)

2000년 : 아주대학교 정보및컴퓨터공학부 졸업 (학사)
2002년 : 아주대학교 정보통신전문대학원 졸업 (석사)
2005년 : 고려대학교 정보보호대학원 졸업 (박사)

2004년～2005년: University of Minnesota 방문연구원
2005년～2011년: 삼성전자 통신·DMC 연구소 책임연구원
2017년～2018년: Illinois Insitute of Technology 방문교수
2011년～현　재: 아주대학교 소프트웨어융합대학 사이버보안학과 교수
※관심분야 : Digital Forensics, ICS/SCADA Security, Anomaly Detection