PETYA RANSOMWARE ANALYSIS REPORT

[MALWARE ANALYSIS REPORT]

Feb, 2017

By WOODONGGYU

목 차

1. 개요

1-1. 배경

Petya 랜섬웨어는 2016년 3월부터 발견된 랜섬웨어로, 기존의 랜섬웨어와 달리 MBR 영역을 변조한다. 이후 강제로 종료 에러를 발생시켜 재부팅을 하게 만드는데, MBR 변조로 인해 정상적인 부팅이 되지 않는다.

타 랜섬웨어와 달리 MBR 영역을 변조하여 부팅을 불가능하게 만든다는 점에서 더 파괴적인 기능을 할 것으로 보이지만, 데이터를 암호화하지 않고 MBR 영역 또한 재 복구가 가능하다. 다만 이러한 형태의 랜섬웨어가 업데이트되어 유포 될 경우 더 큰 피해를 야기할 수 있기에 사용자들의 주의를 요구한다.

본 보고서에서는 Petya 랜섬웨어에 대해 분석하여 기술한다.

1-2. 공격 과정

일반적으로 랜섬웨어의 공격 과정은 <Figure 1>과 같지만, Petya 랜섬웨어에서는 "파일 암호화" 대신 "MBR 영역"을 암호화하여 감염된 사용자의 정상적인 부팅을 불가능하게 한다.

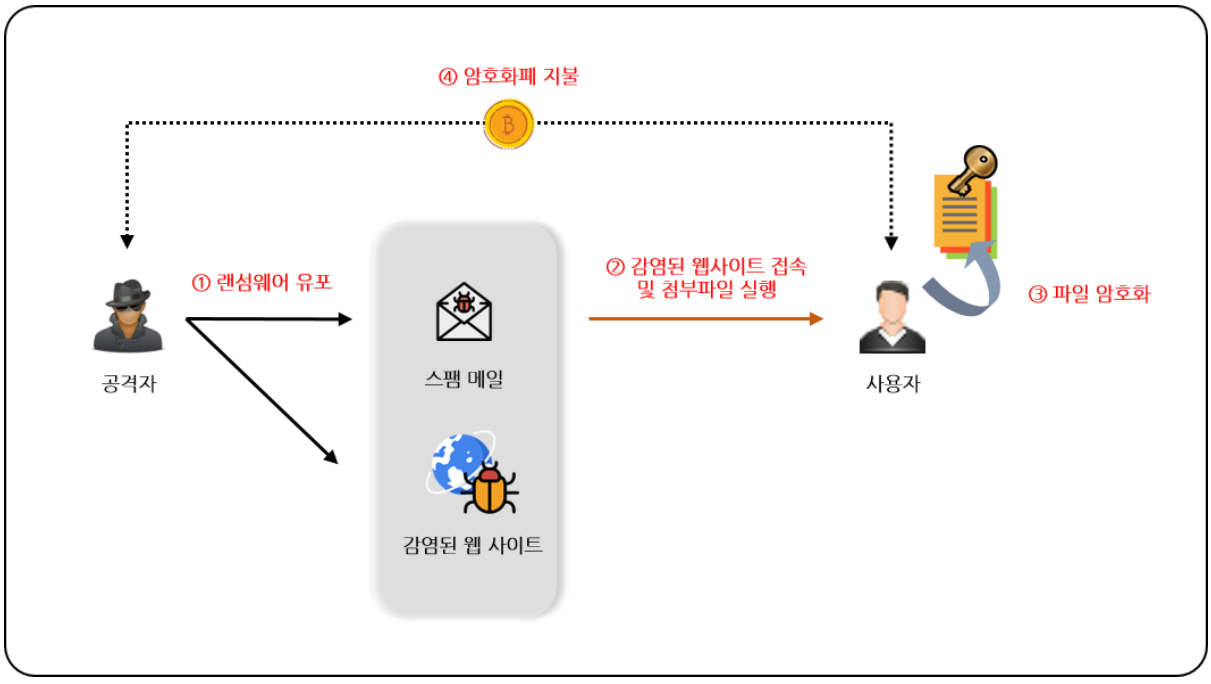

Figure 1. 랜섬웨어 공격 과정

2. 분석

2-1. 악성코드 정보

파일명	Petya.exe
파일 타입	WIN32 EXE
크기	230,912 bytes
해쉬	af2379cc4d607a45ac44d62135fb7015

2-2. MBR(Master Boot Record) 암호화

Petya 랜섬웨어의 경우 원본 데이터가 0x37 의 값과 xor 연산을 통해 데이터 암호화(?)를 수행하기 때문에 상세하게 분석하지 않는다. <Figure 2> 는 최종적으로 암호화 된 MBR 영역의 모습이다.

Figure 2. 암호화 된 MBR 구조

2-3. PC 재 부팅

PC 의 재 부팅을 위한 적절한 권한("SeShutdownPrivilege")을 얻어오고, 하드디스크 에러를 유발하여 PC 가 재 부팅 되도록 한다. 재 부팅 시, 정상적으로 부팅이 이루어지지 않고 <Figure 4>과 같은 랜섬노트를 띄운다.

```
v0 = GetCurrentProcess();
if ( !OpenProcessToken(v0, 0x28u, &TokenHandle)
  || (LookupPrivilegeValueA(0, "SeShutdownPrivilege", NewState.Privileges),
      NewState.PrivilegeCount = 1,
      NewState.Privileges[0].Attributes = 2,
      AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0, 0, 0),
      GetLastError()) )
{
  result = 0;
}
else
{
  v2 = GetModuleHandleA("NTDLL.DLL");
  NtRaiseHardError = GetProcAddress(v2, "NtRaiseHardError");
  (NtRaiseHardError)(STATUS_HOST_DOWN, 0, 0, 0, 6, &v5);
  result = 1;
}
```

Figure 3. PC 재 부팅

```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/PygYgS
   http://petya5koahtsf7sv.onion/PygYgS

3. Enter your personal decryption code there:

   37NrpF-E9Vff3-JLHbJx-J9J53b-khUJzq-ZoVani-bSTj6V-oaGbUq-gtF2RN-HDQAg6-
   YnhJtU-gzhBQH-yrMg3o-qnXDuR-i2nd1D

If you already purchased your key, please enter it below.

Key:
```

Figure 4. 랜섬노트

3. 결론

Petya 랜섬웨어는 암호화 모듈이 아닌, XOR 연산을 통해 암호화를 수행하였기에 검색을 통해 쉽게 복구할 수 있는 도구를 구할 수 있다.

3-1. 대응방안

랜섬웨어는 감염된 이후에는 파일 복호화가 거의 불가능하다. 따라서 감염 피해를 최소화하기 위해서는 미리 예방하는 것이 중요하다. 예방 및 피해 최소화 방안은 아래와 같다.

- *불분명한 메일의 첨부파일 및 링크 실행을 자제한다.*
- *주기적인 백업을 한다. -> 감염 피해를 최소화할 수 있다.*
- *OS 및 사용 중인 S/W 제품에 대해 주기적으로 보안 업데이트를 확인한다.*
- *백신 프로그램을 설치한다.*