

한국정보보호학회 충청지부

제 23회 정기총회 및 정보보호학술논문발표회

2019년 10월 18일 – 19일
대전, 한남대학교(공과대학-9호관)

Organized by

한국정보보호학회 충청지부



대신정보통신(주)



2. 국내 정보보호 연구 경향 분석 - KCI 등재학술지 논문을 중심으로
- 송민경, 김동희, 김소정 (국가보안기술연구소)
3. 타임스탬프 위변조 도구에 의한 안티포렌식 기법에 대한 대응방안(안티-안티포렌식)
- 조규상
4. 블록체인과 Deep Learning을 활용한 악성코드 탐지의 관한 연구
- 최용철, 이덕규 (서원대학교)
5. 블록체인을 활용한 공간공유 시스템에 관한 연구
- 송지훈, 황용운, 이임영 (순천향대학교)
6. 스마트 스피커 환경에서 중간자 공격을 이용한 음원 불법 추출 방안
- 유영웅, 최슬기, 곽진 (아주대학교)
7. 블록체인을 이용한 앱 미터기에서의 요금 산정 기법
- 권용빈, 권혁동, 장경배, 서화정 (한성대학교)
8. 블록체인 확장성 개선을 위한 오프체인과 프라이빗 스마트 컨트랙트 연구
- 김혜빈, 정병규, 신상욱 (부경대학교)
9. **류크 랜섬웨어 동작 과정 분석**
- 김의진, 박소희, 정해선, 곽진 (아주대학교)
10. 블록체인 기반 수소차와 수소 충전소 관리
- 심민주, 권혁동, 서화정 (한성대학교)
11. 원전 네트워크 보안성 강화를 위한 광전송설비 보안기술 연구
- 최호영, 김태훈, 이종진, 김성철
12. 실제 분장이 가능한 딥러닝 기반 얼굴인식 모델 기만공격
- 류권상, 최대선 (공주대학교)
13. 4차식 모듈러스 NTT를 이용한 LAC 구현
- 이주엽, 김수리, 홍석희 (고려대학교)
14. QR 코드 기반의 효율적인 이미지 보호 기법 설계
- 김영세, 김건우 (한국전자통신연구원)
15. 국가사이버안보전략의 기술과제 분포 분석
- 유영인, 배선하, 김소정 (국가보안기술연구소)

류크 랜섬웨어 동작 과정 분석

김의진*, 박소희**, 정해선**, 곽진***

*,***아주대학교 사이버보안학과

**아주대학교 컴퓨터공학과 정보보호응용및보증연구실

An Analysis of Ryuk Ransomware Operating Process

Eui-Jin Kim*, So-Hee Park**, Hae-Seon Jeong**, Jin Kwak***

*,***Department of Cyber Security, Ajou University.

**ISAA Lab., Department of Computer Engineering, Ajou University.

요약

랜섬웨어란 악의적인 공격자가 피해자 컴퓨터 내부에 있는 중요 정보들을 암호화하고, 이에 대한 몸값을 요구하는 악성 소프트웨어이다. 2018년 8월 미국에서 류크 랜섬웨어의 등장으로 조지아 주의 Jackson County 주의 공공업무가 마비되어 피해를 입었으며, 이를 복구하기 위해 40만 달러를 지불하였으나 완벽한 복구가 이뤄지지 않았다. 국내에서는 아직 피해 사례가 보고되지 않았으나, 류크 랜섬웨어의 주요 공격 목표가 기업이나 공공기관이기 때문에 이를 대비할 필요가 있다. 따라서 본 논문에서는 Emotet과 TrickBot을 이용한 류크 랜섬웨어의 동작 과정을 분석한다.

I. 서론

랜섬웨어란 공격자가 피해자 컴퓨터 내부의 정보를 암호화하고 이에 대한 몸값을 요구하는 악성 소프트웨어이다[1].

2018년 8월 류크 랜섬웨어의 등장[2]으로 여러 공격이 일어났으며, 미국의 Jackson County는 랜섬웨어의 공격으로 공공업무 대부분이 마비되었다[3]. 공격에 사용된 류크 랜섬웨어는 TrickBot을 이용해 네트워크 내부를 장악하고, TrickBot을 다운로드하기 위한 드로퍼로 Emotet이 사용되었다[4].

본 논문에서는 2장에서 류크 랜섬웨어와 TrickBot, Emotet에 대해 설명하고, 3장에서 류크 랜섬웨어의 동작 과정을 분석한 뒤, 4장에서 결론을 맺는다.

II. 관련연구

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2017R1E1A1A01075110).

2.1 TrickBot

TrickBot은 뱅킹 트로이 목마의 한 종류로 네트워크를 통해 확산된다. TrickBot의 C&C는 무선 라우터에 설치되며, 감염된 내부 네트워크에서 완벽히 제거하지 않으면 SMB(Server Message Block) 프로토콜 취약점(MS17-010)을 이용해 재발할 수 있다. TrickBot은 피싱을 이용한 악성메일을 통해 주로 퍼지며 네트워크 및 사용자 Credential을 탈취한다[5].

2.2 Emotet

Emotet은 뱅킹 트로이 목마의 한 종류로, 주로 스팸 메일을 이용한 공격을 사용한다. Emotet은 SMB 프로토콜 취약점을 통해 네트워크 및 사용자 Credential, 또는 패스워드를 탈취한다. 공격자들은 메일 내에 Word 문서를 다운로드하게 한 뒤, 문서 내부에 삽입된 난독화된 매크로를 사용하여 공격한다[6].

2.3 Ryuk Ransomware

류크 랜섬웨어는 RDP(Remote Desktop

Protocol) 취약점(CVE-2019-0708)과 SMB 프로토콜 취약점을 이용해 사용자 Credential을 탈취하고, 네트워크에 공유되는 파일들이나 컴퓨터 파일 시스템을 암호화한다. 류크 랜섬웨어는 Emotet과 TrickBot을 이용하여 사용자의 PC에 침입한다[4].

III. 동작 과정

본 장에서는 Emotet과 TrickBot을 이용한 류크 랜섬웨어 동작 과정에 대해서 설명한다.

Step 1. Download Emotet

공격자는 매크로가 삽입된 Word가 있는 스팸메일을 통해 공격하는데, 사용자가 이를 실행하게 되면 PowerShell이 실행되어 Emotet C&C와 통신하여 Emotet을 다운로드 할 수 있다[6].

Step 2. Download Autorun Registry

Emotet은 Autorun 레지스트리를 다운로드하여 윈도우 내부에서 계속해서 작동할 수 있게 한다[6].

Step 3. Download Trickbot Payload

Emotet에 감염된 사용자의 PC는 TrickBot 페이로드를 다운로드하여 사용자 PC내의 Process를 감염시킨다. 이 때 TrickBot은 SMB취약점을 이용해 내부 네트워크에 존재하는 PC로 퍼져 나가게 된다[4,6].

Step 4. Access User's PC and Download Exploit Tool

이렇게 TrickBot에 감염된 PC에 공격자는 네트워크를 제어 할 수 있게 되는데, 공격자는 장악한 네트워크를 이용하여 PowerShell Empire, Cobalt Strike와 같은 Exploit Tool을 다운로드 할 수 있다[2,4].

Step 5. Monitor User's Credential

TrickBot에 감염된 PC를 공격자가 Credential을 Monitoring한다[4].

Step 6. Encrypt Files

공격자는 중요정보들을 선별한 뒤, 류크 랜섬

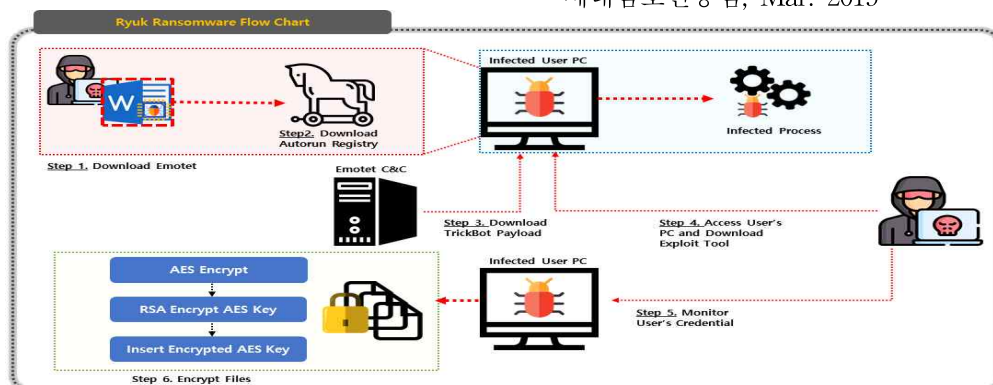
웨어를 통해 암호화한다. 류크 랜섬웨어는 암호화 할때 AES-256을 통해 사용자의 중요 정보들을 암호화한다. 그 후 AES의 키를 RSA 공개키로 암호화, 암호화된 RSA개인키와 공개키는 랜섬웨어 내부에 삽입된다. 모든 과정이 진행된 후 암호화된 파일에 암호화된 AES키가 삽입된다[7].

IV. 결론

본 논문에서는 Emotet과 TrickBot을 이용한 류크 랜섬웨어의 동작 과정에 대하여 분석하였다. 류크 랜섬웨어는 아직까지 복호화 방법이나 복구 툴이 존재하지 않는다[7]. 따라서 류크 랜섬웨어에 대한 지속적인 연구와 이에 대한 대응방안이 필요하다.

[참고문헌]

- [1] Kassner, Michael, "Ransomware : Extortion via the Internet", Tech Republic, Jan. 2010
- [2] FBI FLASH, "Indicators of Compromise Associated with Ryuk Ransomware", FBI, May. 2019
- [3] Joe Stanganelli, "Jackson County Still Recovering After Paying Ryuk Ransom", Security Now, Mar. 2019
- [4] Noa pinkas, Lior rochberger, Matan zatz, "Triple Threat : emotet deploys trickbot to steal data & spread ryuk", Cybereason nocturnus, Apr. 2019
- [5] Malwarebytes, "TrickBot Emergency Kit", Malwarebytes Nov. 2018
- [6] Ahnlab, "Emotet Returns to Prey on Banking Information", ASEC Report Q3, 2017
- [7] 한국인터넷진흥원 , "랜섬웨어 동향보고서", 차세대암호인증팀, Mar. 2019



[그림 1] Ryuk Ransomware 동작 과정