월간 악성코드 분석 보고서 (2018-02)

UBoat Rat 분석 보고서

수산INT 기술 연구소 (CERT)

2018. 02. 01

은닉 악성코드 "Uboat RAT"을 분석한 보고서입니다.
본 문서는 수산아이앤티 CERT에서 작성되었으며 연구 목적의 활용은 가능하나, 그 외 활용으로 인해 발생하는 문제에 대한 법적 책임은 당사자에 있음을 알려드립니다.

문의처: 기술 연구소 CERT
(SungMin.Rue@soosan.co.kr / KimNamGuy@soosan.co.kr / MinKyum89@soosan.co.kr)

SOOSAN INT

목 차

1. 개 요

'지능형 지속 공격 (APT)'는 지능적인 방법을 사용해서 지속해서 특정 대상을 공격하는 것을 말합니다. 과거의 불특정 다수를 노렸던 공격과는 달리, APT 공격은 하나의 대상을 목표로 정한 후에 내부로 침입에 성공할 때까지 다양한 IT기술과 공격방식을 기반으로 여러 보안 위협을 생각하여 공격을 멈추지 않는 것이 특징입니다.

유보트 랫 (UBoat RAT)은 2017년 5월에 발견된 악성코드로 APT 공격 목적으로 사용된 것으로 보입니다. Uboat RAT은 윈도우 업데이트 기능에서 사용되는 컴퓨터 간에 파일을 전송하는 서비스인 마이크로소프트 윈도우 BITS[1]를 사용해 지속성을 실현하는 특징을 가지고 있습니다. 이는 재부팅 후에도 시스템에서 계속 실행되도록 합니다.

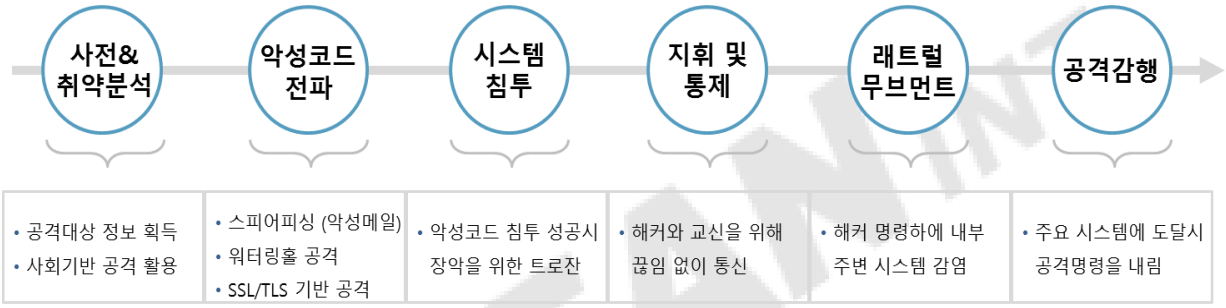
분석한 악성 파일의 이름은 '2017년 연봉 인상 문의 사항 관련 피드백 조사.exe'라는 형태로 한국어를 사용하여 공격 대상을 한국의 인사 담당자를 목표로 둬 배포한 것으로 보입니다. 해당 악성 파일은 VMWare, VirtualBox 등 가상화 소프트웨어를 탐지해 해당 조건에는 실행하지 않도록 하는 조건으로 제작되었습니다. 이는 보안 분석을 어렵게 해 잠복에 적합한 악성코드라고 할 수 있습니다. 피해를 주는 행위를 하지는 않지만, 추가 악성코드 감염 경로로 활용될 수 있어 잠재 위협은 매우 높아 보입니다.

1) BITS (Background Intelligent Transfer Service): 네트워크 연결이 끊어지거나 컴퓨터가 다시 시작되는 등의 이유로 인해 전송 세션이 중단된 경우 파일 전송을 자동으로 재개시키는 기술

2. APT 공격과 Uboat RAT

Uboat RAT은 은닉 악성코드로 APT 공격을 위해 만들어진 것으로 보입니다. Uboat RAT 자체가 위협적이지 않지만, APT 공격용으로 제작된 것으로 보여 큰 위협이 있을 것으로 보입니다. Uboat RAT의 위험성을 알기 위해 APT 공격과 Uboat RAT을 살펴보도록 하겠습니다.

2.1 사이버 킬 체인 (APT 공격 프로세스)[2), 3)]



사전&취약분석 (Reconnaissance)

공격 대상의 정보를 수집해서 어떤 경로로 침투할 수 있을지 전략을 구성하는 단계로 APT 공격의 성공 여부를 결정짓는데 가장 중요한 단계입니다. APT 공격의 주요 목표 시스템들은 기관에 중요 역할을 하고 있어 보안이 철저합니다. 그래서 철저한 보안 시스템을 뚫기 위해 해킹하기 쉬운 주변의 시스템들을 먼저 해킹하고 점차 권한을 획득하면서 목표 시스템에 도달하는 전략을 '사회공학기법'이라고 합니다. 대부분 APT 공격은 사회공학 기법을 많이 활용 합니다.

사회공학기법의 가장 중요한 점은 목표시스템의 이해관계자를 파악하는 것입니다. 이러

2) 한국정보화진흥원 (2016), "4차 산업혁명과 사이버 보안대책", 지능화연구시리즈

3) Ping Chen, and etc (2014)., "A Study on Advanced Persistent Threats)", International Federation for Information Processing.

한 경우 해커들은 OSINT(Open Source Intelligence Tool)를 주로 사용합니다. OSINT는 사이버의 공적인 영역에서 이용 가능한 정보를 말합니다. 페이스북에 업데이트된 개인정보, 학회 컨퍼런스에 올라와 있는 개인 약력들 등이 모두 OSINT에 해당합니다.

악성코드 전파 (Weaponization)

악성코드로 감염시킨 첨부파일을 SNS 및 이메일로 보내 취약한 시스템에 전달하는 것으로, 이때 악성코드를 전달하기 위한 가장 대표적인 방식은 '스피어피싱' 공격입니다. 피싱이 다수를 목적으로 한다면 스피어피싱은 명확한 대상에게 이와 같은 공격을 감행하는 것을 뜻합니다. 스피어피싱 이외에도 해커가 OSNIT조사를 기반으로 공격대상이 자주 방문하는 사이트를 파악한 뒤 자주 방문하는 사이트에 악성코드를 심어 놓고 대상자가 방문할 때 감염시키는 워터링홀 기법도 자주 이용됩니다.

시스템 침투 (Delivery)

해커가 처음으로 시스템 접근 권한을 획득한 것을 의미합니다. 목표대상 시스템에 성공적으로 악성코드를 설치하면 '시스템 침투' 단계를 성공적으로 마친 것이지만 사용자가 첨부파일을 열어보지 않고 스팸으로 처리하거나 보안 프로그램 때문에 감지할 경우 '시스템 침투' 단계는 실패가 되는 것입니다. 악성코드가 시스템 접근 권한을 무사히 획득하였다면 악성코드는 트로잔과 같은 악성코드를 시스템에 심어 놓고 은닉합니다.

지휘 및 통제 (C&C: Command and Control)

악성코드는 해커와 끊임없이 현재 상태 정보를 주고받는 단계입니다. 이 단계는 보안시스템에 의해서 탐지될 위협이 높은 단계이므로, 탐지를 회피하기 위한 현재 상태를 블로그 사이트에 업데이트하거나 SNS의 메시지의 형태로 업데이트하는 수법을 사용합니다. 이외에도 네트워크 통신을 숨기기 위해서 원격제어 프로그램을 사용하거나, 익명 네트워크 및 토르와 같은 익명 브라우저를 사용하기도 합니다.

래트럴 무브먼트 (Lateral Movement)

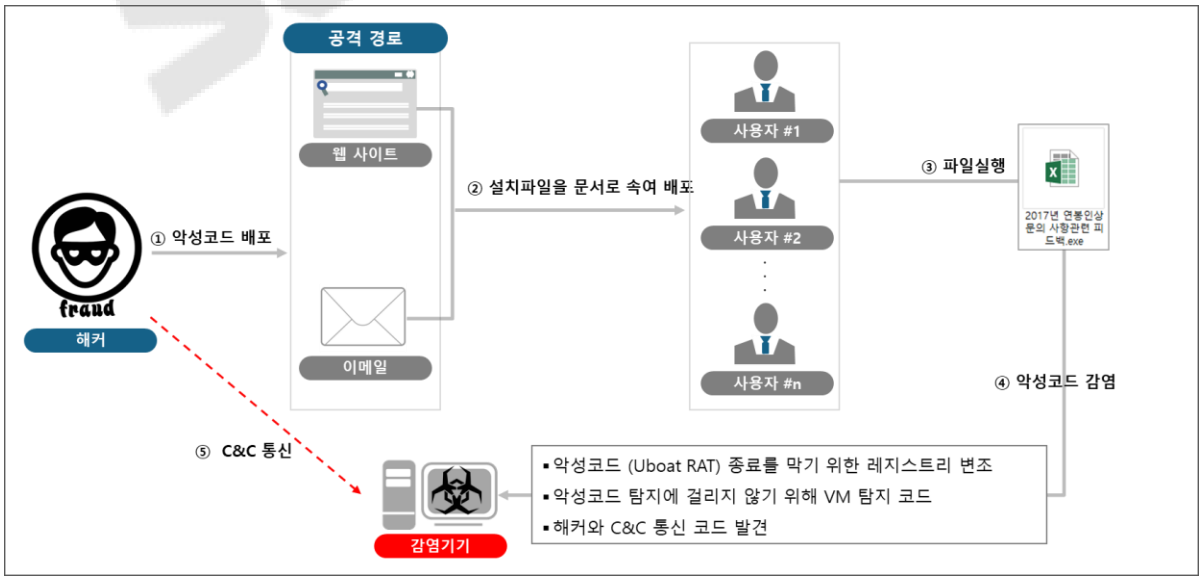
C&C 채널 구축 후에 해커는 악성코드에 명령을 내려 내부 네트워크와 주변 기기들을 감염시키도록 명령을 내리는 단계입니다. 악성코드는 활동 할 수 있는 권한을 점차 획득해 최종 목표 시스템까지 접근하게 됩니다. 이 단계에서 해커는 3가지 활동을 수행합니다. 첫째 현재 감염시킨 시스템에서 목표 시스템까지 어떻게 접근해야 할지에 대한 로드맵을 구상합니다. 둘째 주변 시스템들을 보안 운영자에게 들키지 않고 해킹 할 수 있는 방법을 구상합니다. 마지막으로 지금까지 해킹한 시스템에서 해커가 취할 수 있는 중요 정보자산들이 무엇이 있는지 파악합니다.

공격감행 (Actions on Objectives)

최종 목표 시스템에 도달했으면 적절한 시기에 맞추어 사이버 공격을 가하는 최종 단계입니다. 보통 해커가 공격 신호를 보낼 때 SSL/TLS 혹은 Tor와 같은 보안 프로토콜을 사용해 보안시스템의 감시망을 피해서 공격명령을 내리는 경우가 많습니다.

2.2 APT 공격 관점에서의 Uboat RAT

Uboat RAT의 행위는 아래 그림과 같습니다.



2.2.1 공격경로

공격 경로를 분석한 결과, 해커는 2가지 방법으로 Uboat RAT을 전파하고 있습니다. 해커는 '워터링 홀' 수법을 이용해 Uboat RAT을 전파할 수 있습니다. 워터링 홀은 사이트에 악성코드를 심어서 방문자를 감염시키는 방법입니다. 두 번째 방법으로는 악성 이메일을 이용하는 것입니다. 실행 파일을 문서 형태로 위장시켜 Uboat RAT 설치파일을 유포하는 것입니다. 사용자가 다운 후에 실행하면, Uboat RAT 기능이 기기에 몰래 작동하게 됩니다

2.2.2 악성코드 위험성 (감염증상)

Uboat RAT은 C&C 기능 이외에 발견된 악성 행위는 없었습니다. 다만 악성코드 탐지를 피하고자, 패킹과 VM 탐지 우회 기술이 적용돼 있습니다. 이는 APT의 시스템 침투부터 래트럴 무브먼트를 위한 것으로 볼 수 있습니다. 이유는 아래와 같습니다.

1. 패킹과 VM 탐지 우회 기술은 보안 솔루션에 탐지를 어렵게 합니다. 이는 시스템 침투와 래트럴 무브먼트 성공률을 높입니다.
2. APT는 잠복해 있다가 중요 시스템에 접근했을 때 공격을 가하는 경우가 많습니다. 해당 파일 또한 이러한 용도로 만들어진 것으로 보입니다. 아무런 악성 행위를 하지 않고 잠복해 있다가, C&C 명령받을 시에 공격을 가할 가능성이 높아 보입니다.

정리하면 Uboat RAT이 직접 피해를 주지는 않아 위협적이지 않아 보입니다. 그러나 APT 공격에 적합한 은닉 악성코드이기 때문에 잠재 위협은 매우 높은 것으로 결론을 내렸습니다.

3. 분석 내용 (Uboat RAT)

수산INT CERT에서는 Uboat RAT을 실제로 분석해 보았습니다. 분석 내용을 다음과 같습니다.

3.1 분석 파일 정보

분석 파일명은 "**2017년 연봉인상 문의 사항 관련 피드백 조사.exe**" 입니다.

해당 파일 해쉬 정보는 아래와 같습니다.

- MD5: 02a7993fcd5fea4442271e91e12d2df7
- SHA-1: d1795a10bbd8883e442547634e9a89cf67b8ebd8
- SHA-256: e52d866e5b77e885e36398249f242f8ff1a224ecce065892dc200c57595bb494

해당 파일에서 통신하는 C&C 서버를 발견했습니다. 해당 C&C로 통신을 해 감염 당한 컴퓨터의 정보를 갈취하는 백도어 (Backdoor) 형태의 악성코드가 만들어집니다. 생성 파일 경로의 폴더 (아래 그림 참조)에 악성 파일을 개별로 드롭퍼[4] 시킵니다. .exe의 파일은 "2017년 연봉인상 문의 사항 관련 피드백 조사.exe" 파일을 복사하여 옮긴 파일입니다. ddd.bat 파일의 경우에는 재부팅 후에도 재실행이 가능하도록 하는 레지스트리 변조 및 사용자 권한을 변조하는 행위를 하게 돼 있습니다. 또 Init.bat 파일은 악성파일인 .exe를 계속 실행시키면서 .exe파일이 네트워크 통신을 지속해서 하도록 유지하는 역할을 하고 있습니다.

구 분	악성 행위 문자열 및 생성 파일
C&C	210.205.4.5
생성 파일 경로	C:₩Programdata₩.exe
	C:₩Programdata₩ddd.bat
	C:₩Programdata₩init.bat
레지스트리 변조 코드	Reg add HKEY_CURRENT_USER₩Software₩Classes₩mscfile₩shell₩open₩command /t REG_EXPAND_sz /d %s /f.cmd.exe /c eventvwr.exe

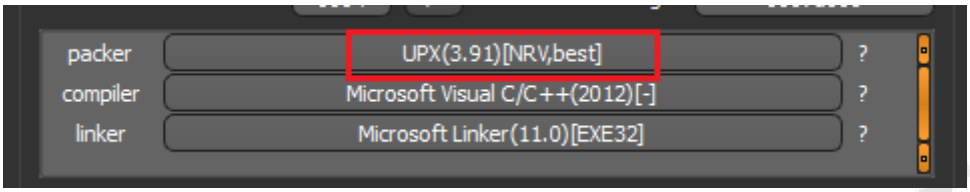
4) 드롭퍼 (Dropper): 악성코드를 설치 하는 역할을 맡은 애플리케이션 혹은 사이트를 말합니다.

3.2 실행 증상

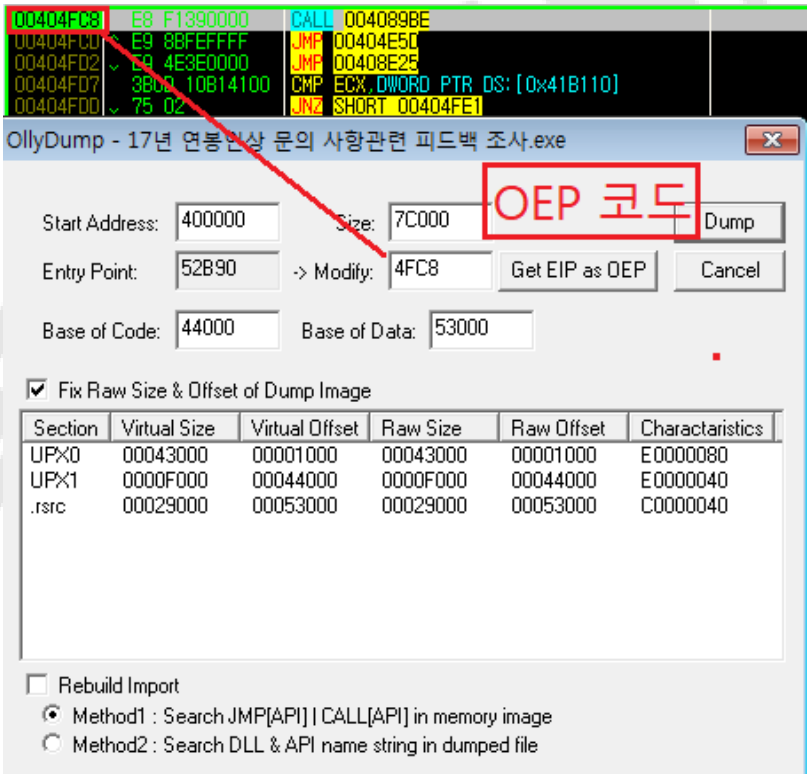
Uboat RAT 은 은닉을 목표로 만들어진 악성코드입니다. 따라서 가상환경 탐지를 우회하는 기능이 있는 것이 특징입니다. 가상환경 우회 탐지 기능과 악성 행위에 대해 알아보도록 하겠습니다.

3.2.1 패킹 (탐지 우회 기능)

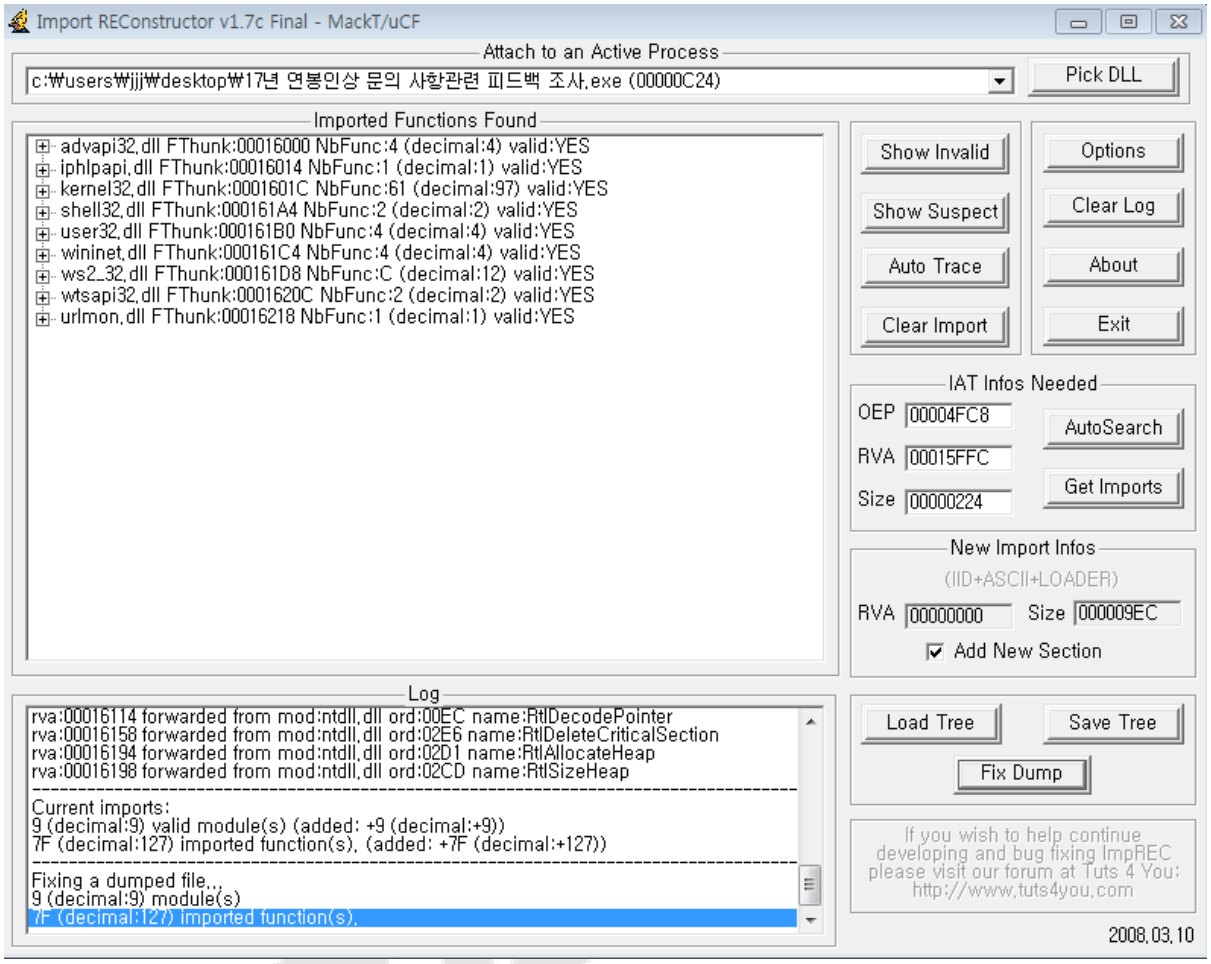
(1) 패킹 확인결과 UPX 3.91 로 패킹 (Packing)이 되어 있음.



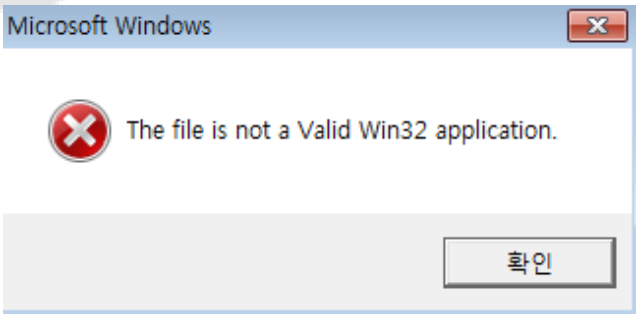
(2) 패킹 된 어셈블리어를 추적하여 OEP(Original Entry Point)를 찾은 후 OEP 구간에서 파일 덤프



(3) 패킹이 해제 된 Dump 파일을 실행 가능하도록 기존의 사용했던 API 들을 재정리



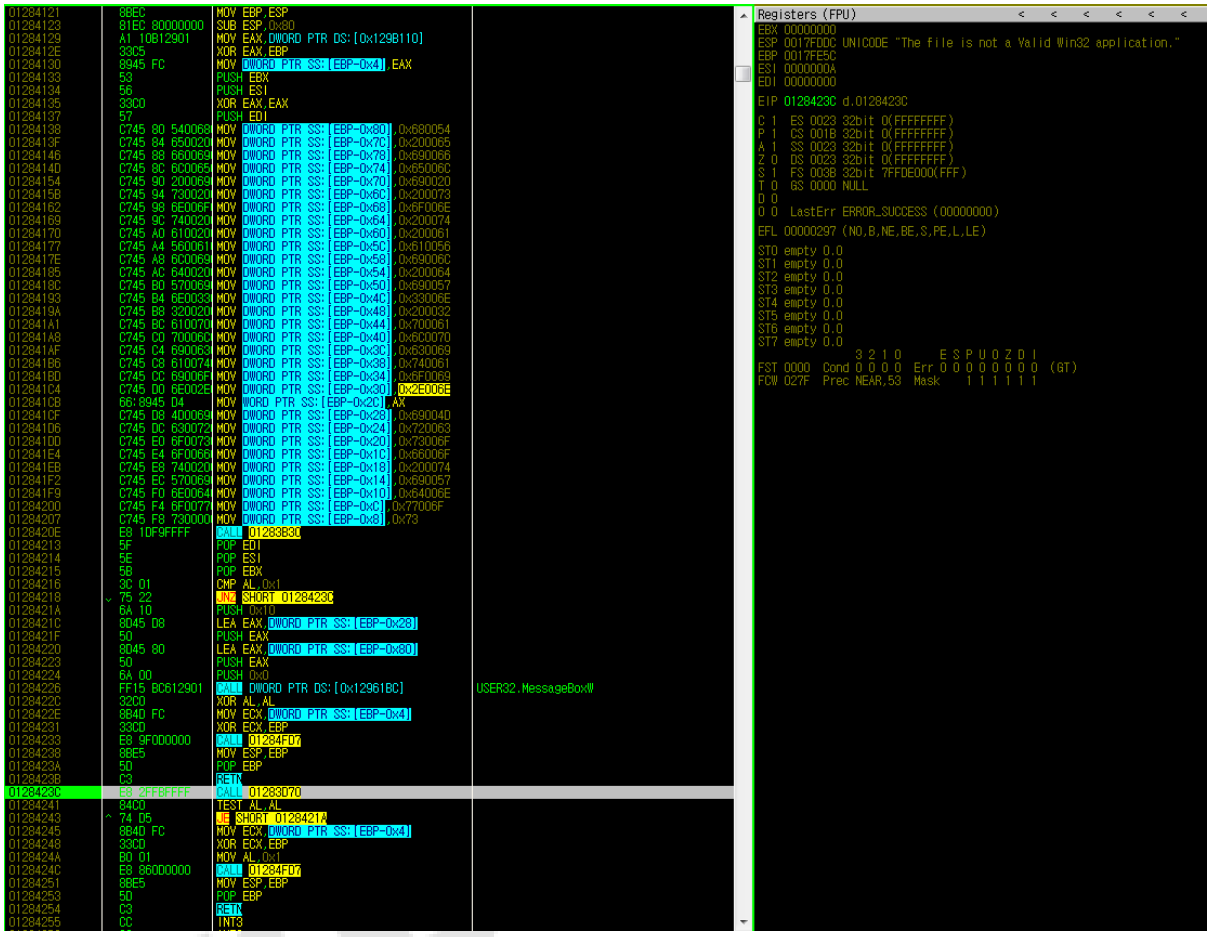
(4) Unpacking 된 파일을 가상환경에서 실행하게 되면 메시지 창이 뜸



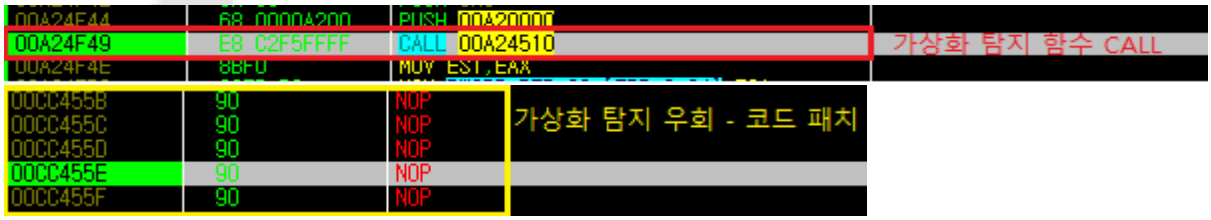
[가상 환경(Virtual Machine) 탐지 실행 중지]

3.2.2 가상환경 (Virtual Machine) 탐지 코드 패치 우회 (탐지 우회 기능)

(1) 해당 구간은 가상 환경(Virtual Machine) 탐지를 하는 알고리즘 구간 (가상화 탐지 함수 내부)



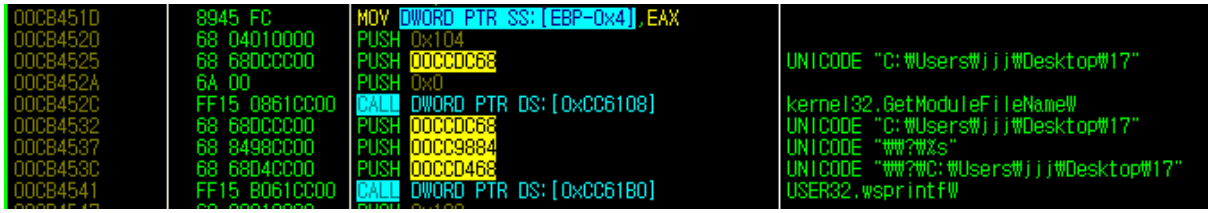
(2) 가상 환경 (Virtual Machine) 탐지 CALL 부분 코드 바이패스 (Code Bypass[5])



5) VM 탐지 시에 우회하게 하는 소스코드

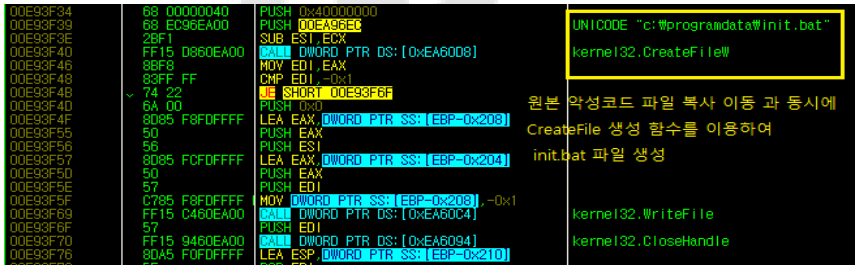
3.2.3 Uboat RAT 악성 행위 분석

(1) GetModuleFileNameW 함수를 사용하여 현재 악성 파일 실행 경로를 불러옴

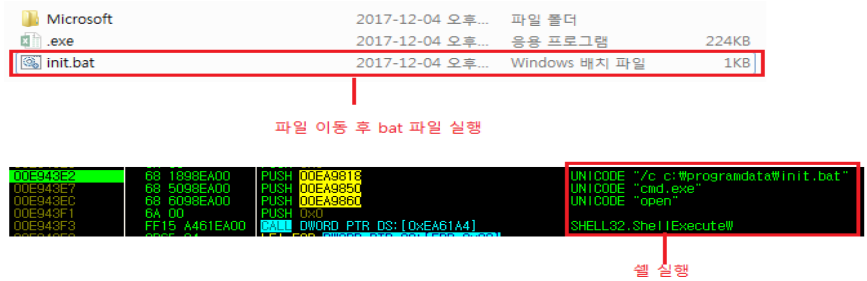


(2) 실행 경로를 이용하여 악성 파일을 CopyFileW 함수를 사용한 후, C:Programdata₩.exe 라는 이름으로 복사

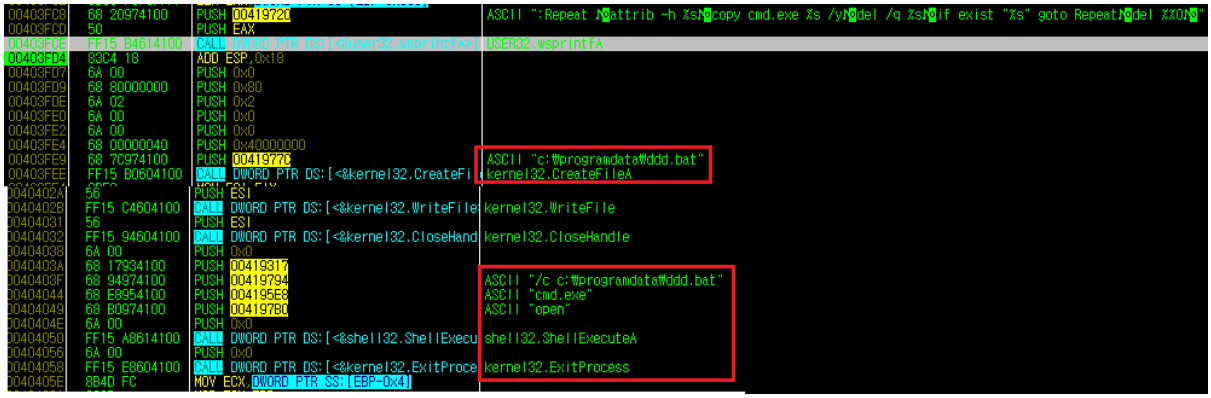
(3) 원본 악성코드 파일이 .exe 이동하는 동시에 Programdata 폴더에 init.bat 이라는 윈도우 스크립트 실행 파일 생성.



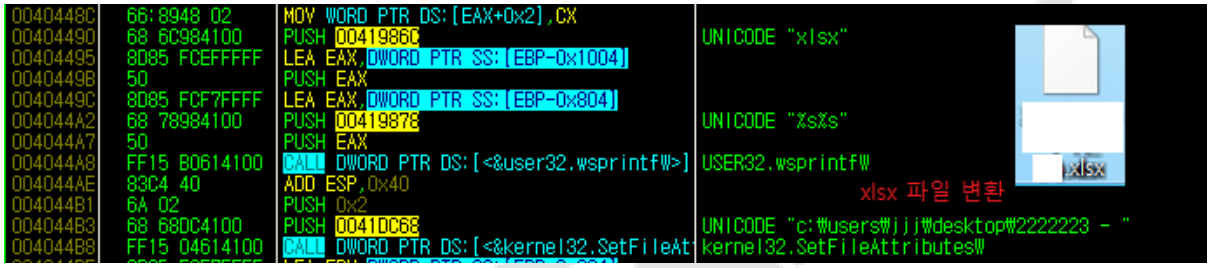
(4) Init.bat 생성 후 자동으로 실행하도록 설계



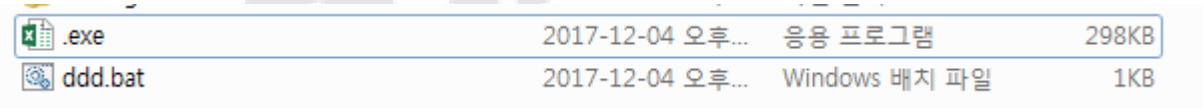
(5) Init.bat 실행 후 자가 삭제 및 ddd.bat 기능은 원본 악성코드를 보이지않게 숨기는 역할



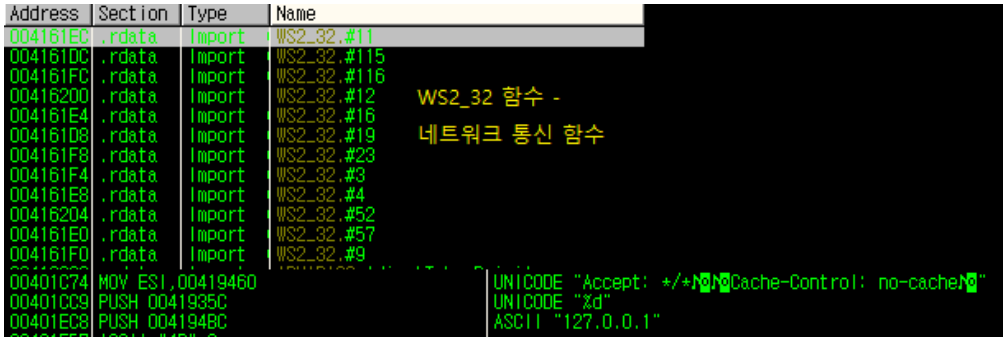
(6) 정상 엑셀 확장자인 .xlsx 파일을 생성 ➔ 의심하지 못하게 .xlsx 파일로 실행된 것처럼 보여줌



(7) 해당 악성 파일은 악성 코드가 지속적으로 실행 되도록 레지스트리를 변조



(8) CMD 창을 이용해 .exe 파일을 실행, 종료를 반복해 공격자 C&C 서버랑 네트워크 통신을 함[6].



6) WS2_32.dll은 네트워크 사용될 때 주로 쓰는 함수 입니다

3.3 대응방안

1. **eWalker 설치로 악성 사이트 접속을 차단합니다.**

   Uboat RAT은 악성 사이트로 배포되는 경우가 많습니다. 따라서 악성 사이트에 접속하지 않는 것이 가장 중요한 예방법입니다. 그런데 문제는 악성 사이트를 탐지하는 것은 쉽지 않습니다. 자사에서 제공하는 eWalker 제품은 40만 개가 넘는 악성 URL을 보유하고 있습니다. 이를 활용하면, 쉽게 워터링 홀로 인한 감염을 예방할 수 있습니다. 아울러 Uboat Rat의 C&C 도메인의 경우, eWalker에서 이미 차단하고 있습니다. 이는 Uboat RAT으로 인한 2차 피해를 막을 수 있게 합니다.

2. **의심되는 메일을 열지 않는 것도 중요한 예방법입니다**.

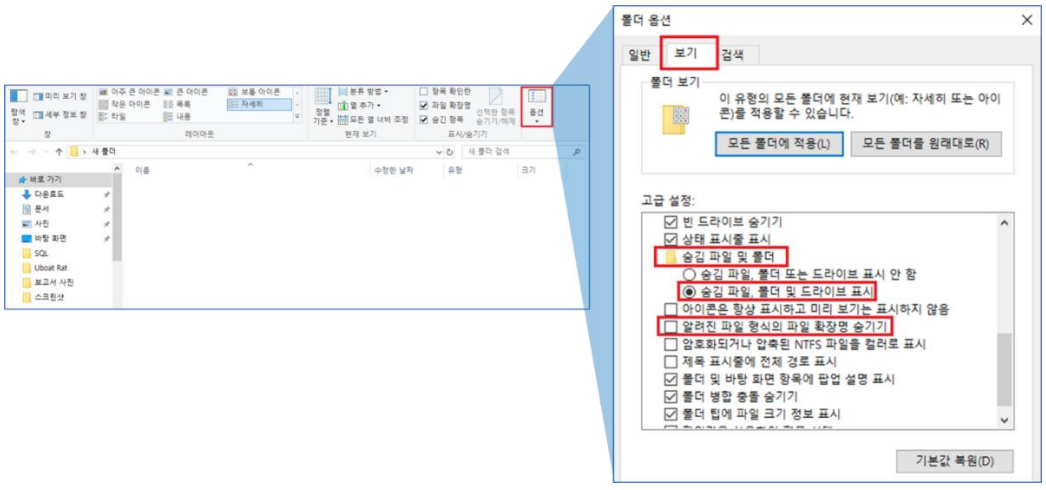
   출처를 알 수 없는 메일에는 악성코드를 숨겨놓을 가능성이 높기 때문입니다.

3. **백신과 OS를 정기적으로 업데이트 하는 것도 중요한 예방법입니다.**

   은닉 악성코드 감염 방지를 위해 백신과 OS를 설치하는 것도 중요합니다. 다만 알려지지 않은 악성코드인 경우 탐지가 힘듭니다. 이러한 경우 전문가 분석이 필요합니다. **본인이 속한 기관이 은닉 악성코드에 감염됐다고 의심된다면, 저희 보안 연구소에 연락 (QI@soosan.co.kr)을 주셔도 됩니다**

4. **확장자명 설정으로 의심 파일 실행을 방지할 수 있습니다.**

   *.EXE 실행 파일을 아이콘은 문서(Excel, Word) 모양으로 보이게 하여 문서 파일로 위장하는 경우가 있습니다. 이를 예방하기 위해서는 확장자명 설정을 하는 것이 중요합니다. 그렇게 하면 파일 모양 문서로 속여도, *.EXE 임을 파일 이름에서 확인할 수 있습니다.



2018 년 수산 INT 연구 보고서 발간 내역

월간 악성코드 분석 보고서

2018-01 호: 가상화폐 채굴 악성코드 분석 (2018 년 01 월)
2018-02 호: UBoat Rat 분석 보고서 (2018 년 02 월)

감사합니다.

글로벌 네트워크 보안 솔루션 전문기업

SOOSAN INT

서울특별시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)

Tel 02.541.0073 | **Fax** 02.541.0204

E-mail QI@soosan.co.kr

HP http://www.soosanint.com