SPECIAL REPORT

OPERATION MONEYHOLIC

오퍼레이션 머니홀릭 상세 분석

암호화폐 관련 타깃 공격 프로파일링…배후는?

반복적인 등락에도 불구, 암호화폐(Cryptocurrency)에 대한 관심은 여전히 뜨겁다. 가격 상승에 대한 기대와 익명성으로 추적이 어렵다는 점 때문에 공격자들도 암호화폐를 획득하기 위해 랜섬웨어를 비롯해 마이너(Miner, 또는 Coin miner), 크랩토재킹(Cryptojacking) 등 다양한 형태의 악성코드를 제작, 유포하고 있다. 또 암호화폐 거래소 공격이나 암호화폐 사용자 계정 해킹도 심심치 않게 발생하고 있다. 특히 지난 2018년 초부터 국내 암호화폐 거래소와 이용자를 겨냥한 악성코드 공격이 지속적으로 전개되고 있다.

안랩 시큐리티대응센터의 보안분석가들은 일련의 암호화폐 관련 공격을 '오퍼레이션 머니홀릭(Operation Moneyholic)'으로 명명하고, 이에 관한 분석 보고서를 발표했다.

안랩 시큐리티대응센터(AhnLab Security Emergency response Center, ASEC)는 다수의 암호화폐 관련 악성코드를 분석하던 중, 타깃 공격으로 의심되는 일련의 활동을 포착했다. ASEC이 '오퍼레이션 머니홀릭(Operation Moneyholic)'으로 명명한 악성코드 활동과 그 배후 조직(위협 그룹)을 추적 · 분석한 결과, 공격 타깃은 암호화폐 거래소와 이용자로 좁혀졌다. 또한 오퍼레이션 머니홀릭이 수년간 국내에서 타깃 공격을 전개한 특정 위협 그룹과 관련된 정황도 드러났다.

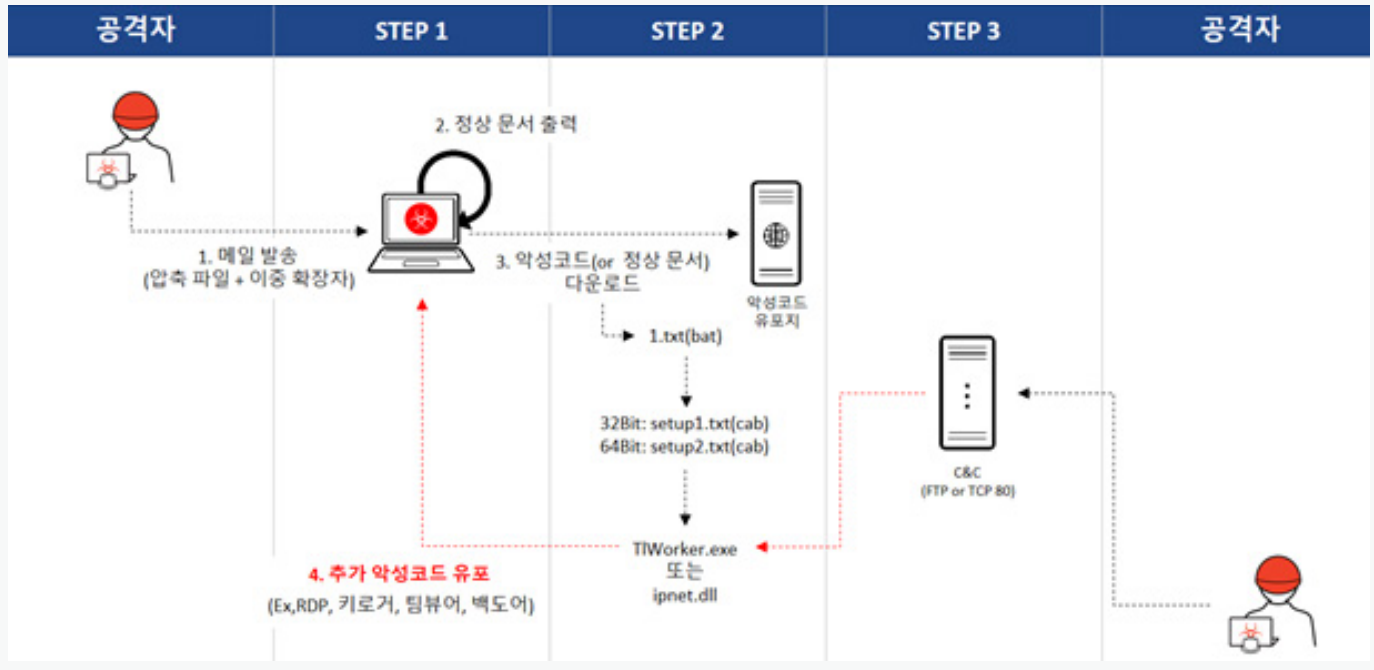
오퍼레이션 머니홀릭은 주로 이메일을 통해 악성코드를 유포하고 있다. 주목해야 할 부분은 오퍼레이션 머니홀릭이 지난 2018년 2월부터 2019년 8월 현재까지 악성코드 제작, 유포 방식을 다양하게 변화시켜 왔다는 점이다. 오퍼레이션 머니홀릭 악성코드의 특징을 시기별로 상세히 살펴보자.

이중확장자와 공백을 이용한 파일명(2018년 초, 중반)

오퍼레이션 머니홀릭은 2018년 초부터 중·후반까지 이메일에 첨부한 파일명에 이중확장자를 사용하거나 의도적으로 공백을 포함했다. 실행 파일인 것을 숨겨 사용자의 의심을 피하기 위한 것으로, [표 1]과 같이 앞부분에 문서 파일 포맷의 확장자명(.xlsx, .hwp 등)을 넣어 문서 파일로 위장하고 있다. 파일명에 암호화폐 관련 내용(코인, BCOT 등)이 포함된 것도 눈길을 끈다.

	파일명
1	WXB 코인　배정 내용 – 송부용.xlsx.　　exe
2	***그룹 3차 –5차 마지막 BCOT 구매 리스트 및 수량계산 확인.hwp.exe

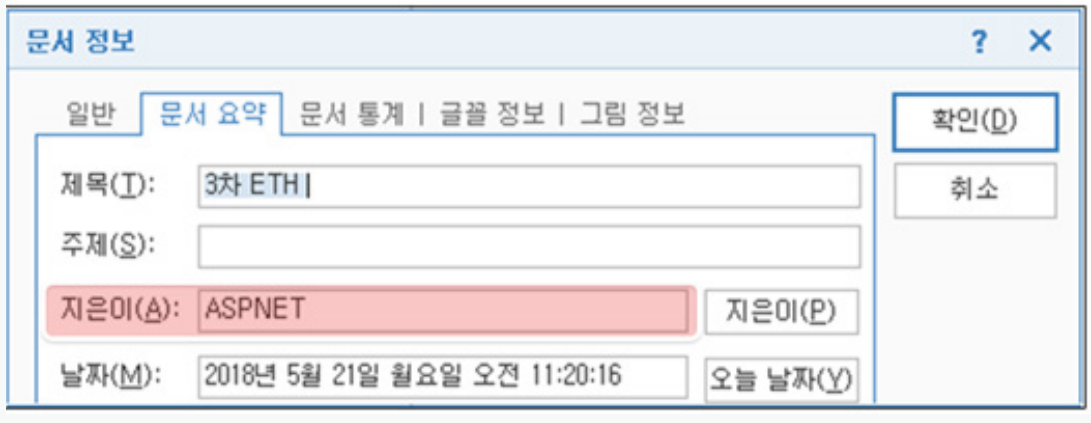
[표 1] 이중확장자 및 공백을 사용한 파일명



[그림 1] 악성코드 동작 과정

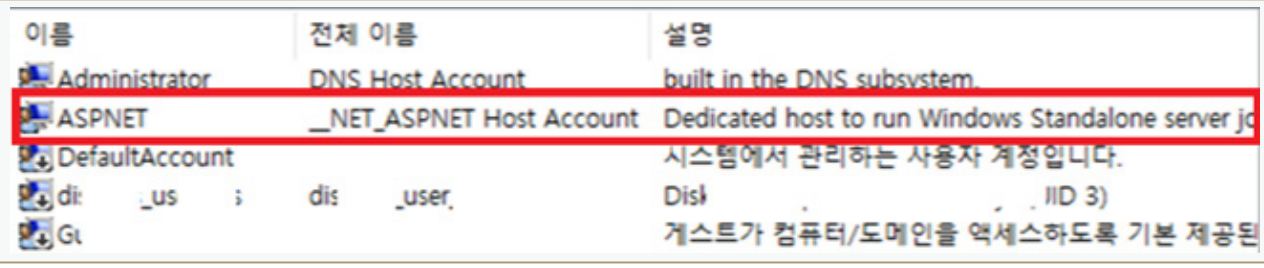
사용자가 문서 파일처럼 보이는 첨부 파일을 실행하면 [그림 1]과 같은 방식으로 악성코드가 동작한다. 첨부된 악성 파일이 실행되면 다수의 악성코드를 추가로 다운로드하는데, 백도어 기능을 수행하는 TiWorker.exe도 함께 다운로드된다. TiWorker.exe는 소스코드가 공개된 중국산 백도어를 기반으로 제작된 것으로, C&C 서버와 통신하며 특정 시그니처(fxftest)를 전송한다.

[표 1]의 한글 문서로 위장한 파일(~BCOT 구매 리스트~.hwp.exe)이 추가 악성코드를 다운로드하는 C&C 서버 주소에는 악성 파일 3개와 함께 사용자의 의심을 피하기 위한 위장용 정상 파일 8개가 존재한다. 위장용 파일 중 BASE64로 암호화되어있는 파일을 복호화하면 암호화폐 이더리움(ETH) 관련 내용의 한글 파일이 나타나는데, 파일의 작성자(지은이) 정보에 'ASPNET'이라는 계정이 사용됐다([그림 2]). 해당 파일 외에 나머지 7개의 위장용 파일을 마지막으로 저장한 사람의 계정도 ASPNET이다. 공격자가 ASPNET 계정으로 로그인 후 위장용 문서 파일 1개로 각기 다른 내용의 문서 파일 7개를 만들었음을 짐작할 수 있다.



[그림 2] 이더리움 관련 내용으로 위장한 한글 파일의 문서 정보

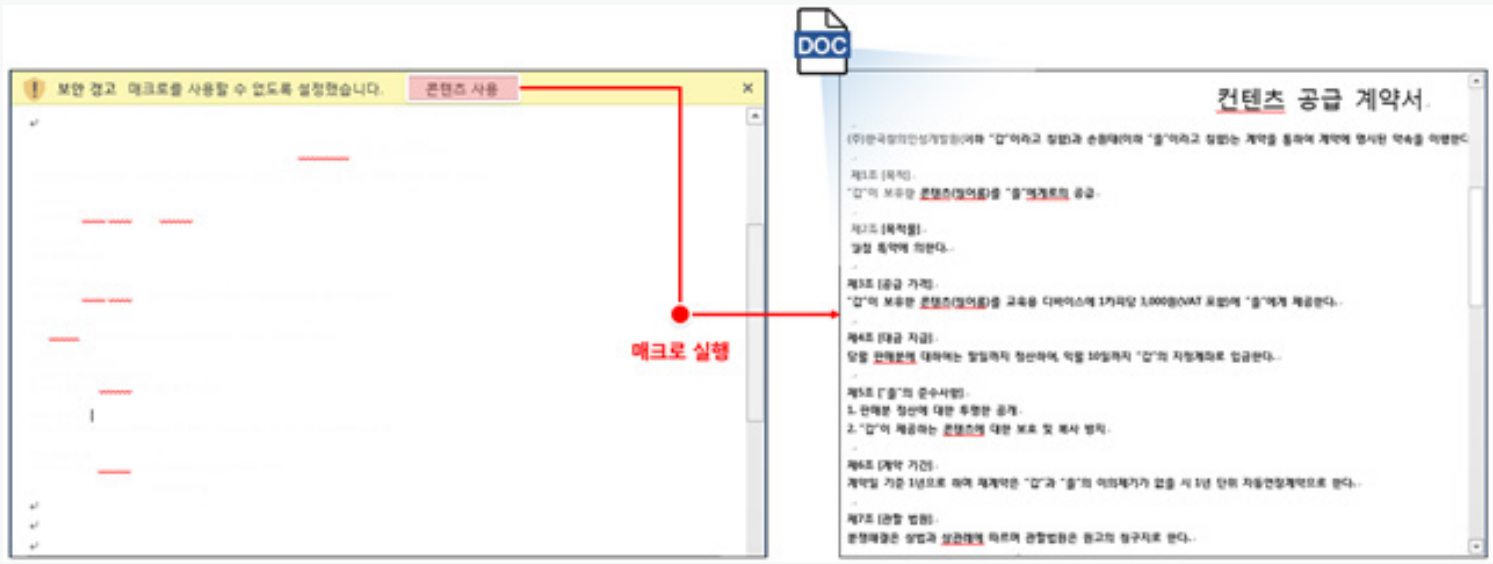
'ASPNET'은 TiWorker.exe가 추가로 다운로드한 악성코드가 감염 PC에 생성한 원격 데스크톱 프로토콜(Remote Desktop Protocol, 이하 RDP) 계정이다. 공격자는 RDP 계정을 통해 외부에서 감염 PC에 접속해 악의적인 행위를 수행할 수 있다. 안랩의 분석 결과, 공격자는 RDP 계정을 통해 감염 PC에 접속한 후 비밀번호를 변경한 것으로 보인다.



[그림 3] 감염 PC에 생성된 RDP 계정(ASPNET)

다양한 기법으로 위장용 문서 파일 제작(2018년 하반기)

오퍼레이션 머니홀릭은 사용자의 의심을 피하기 위해 2018년 후반부터 매크로, 문서 취약점(OLE/Cve-2017-8570 등), 또 MS 워드의 정상 기능인 DDE(Dynamic Data Exchange)를 악용하는 등 다양한 기법으로 위장용 문서 파일을 제작했다. 매크로를 이용한 공격 시 악성 매크로가 포함된 시트를 숨기거나 [그림 4]와 같이 '콘텐츠 사용'을 클릭하도록 유도했다.



[그림 4] '콘텐츠 사용' 클릭 유도를 통한 악성 매크로 실행

이들은 사회공학기법(Social Engineering)을 이용해 공격 성공률을 높였다. 일례로, [그림 5]와 같이 국내를 비롯해 해외에서도 많은 팬덤을 형성하고 있는 아이돌 그룹과 관련된 내용으로 위장한 악성 압축파일을 유포했다.

[그림 5] 유명 아이돌 그룹 관련 내용으로 위장한 악성 파일

아마데이(Amadey) 백도어의 등장(2018년 후반~현재)

2018년 하반기 이후 눈에 띄는 변화가 나타났다. 바로 '아마데이(Amadey)'라고 불리는 봇넷(Botnet)을 사용한 것이다. BASE64로 암호화된 txt 파일(cab 파일)을 복호화하면 아마데이가 포함되어 있는 것을 확인할 수 있다.

아마데이는 러시아 개발자가 제작한 것으로 알려진 봇넷 악성코드로, 공격자는 아마데이 봇넷에 감염된 시스템에 원하는 파일을 다운로드 및 실행하도록 작업 명령을 내리거나 감염 시스템의 정보를 확인할 수 있다.

오퍼레이션 머니홀릭이 유포한 아마데이는 정상 파일처럼 외형을 위장하고 있다. 파일 형태의 외형으로 존재하고 실행되지만, 실제로는 메모리상에서 실행 파일로 재구성되어 백도어 역할을 수행한다. 오퍼레이션 머니홀릭의 아마데이의 외형은 [그림 6]에 붉은색으로 표시된 것과 같은 공통적인 특징을 보이는데, 여기에서 VirtualProtect()로 보호되는 영역에 존재하는 데이터는 암호화된 쉘코드(Shellcode)와 아마데이(Amadey)로 구성되어 있다.

[그림 6] 아마데이 외형의 공통적 특징

오퍼레이션 머니홀릭의 아마데이는 주로 C&C 주소나 백신 프로그램(Anti-virus)의 이름을 문자열로 사용하고있다. 감염 PC에 해당 백신 프로그램이 설치되어 있는지 확인하고, 그 결과를 플래그(Flag)로 설정해 C&C 서버에 전송한다. 전송된 내용은 [그림 7]과 같이 아마데이의 관리자 메뉴의 'AV' 탭에 표시된다.

[그림 7] Amadey 관리자 메뉴에 표시된 감염 PC의 백신 정보

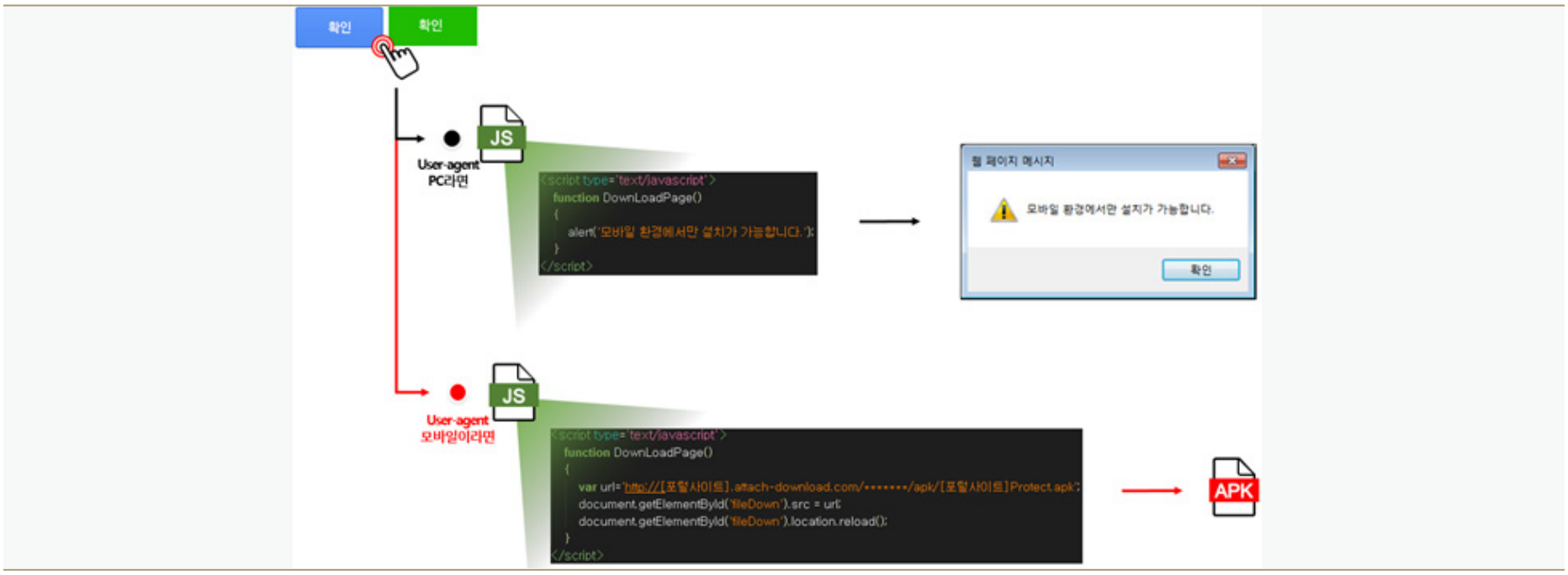
아마데이 변종과 C&C 서버가 통신한 패킷을 분석한 결과, 오퍼레이션 머니홀릭은 감염 PC의 프로세스 목록에 가상 환경과 관련된 프로세스가 실행 중이면 이를 악성코드 분석용 PC로 판단하고 분석을 방해하기 위해 MBR 파괴 악성코드를 추가로 다운로드하는 것이 확인됐다. 감염 PC에 암호화폐 관련 데이터가 존재하면 이를 탈취하는 악성코드를 추가로 다운로드한다.

공격 범위 확대(2019년 상반기)

2019년 5월부터 유포된 악성코드(cab)에는 기존과 같은 백도어(TIWorker.exe, ipnet.dll, Amadey)가 존재하지 않았다. 대신, 운영체제에서 지원하는 콘솔 명령을 이용해 감염 PC의 파일 및 폴더 리스트, 운영체제 및 하드웨어 사양

등의 정보를 수집하는 배치 파일과 수집한 정보를 C&C 서버로 전송하는 실행 파일(Sendfile.exe)이 존재한다.

또 다른 변화는 기존의 윈도우용 악성코드뿐만 아니라 안드로이드용 악성 앱을 제작, 유포하기 시작했다는 점이다. 악성 앱은 윈도우용 악성코드를 유포한 서버에서 발견됐다. 악성 앱이 실행되면 먼저 감염 시스템을 확인하는데, PC 환경일 경우 [그림 8]과 같이 '모바일 환경에서만 설치가 가능합니다'라는 메시지를 노출한다. 안드로이드 스마트폰에 설치된 것으로 확인되면 악성 앱 다운로드 링크로 연결한다. 이를 통해 다운로드된 악성 앱은 사용자의 의심을 피하기 위해 아이콘을 숨긴 후 백그라운드 상에서 정보 탈취 등 악의적인 행위를 수행한다.



[그림 8] 감염 시스템의 환경을 확인하는 악성 앱

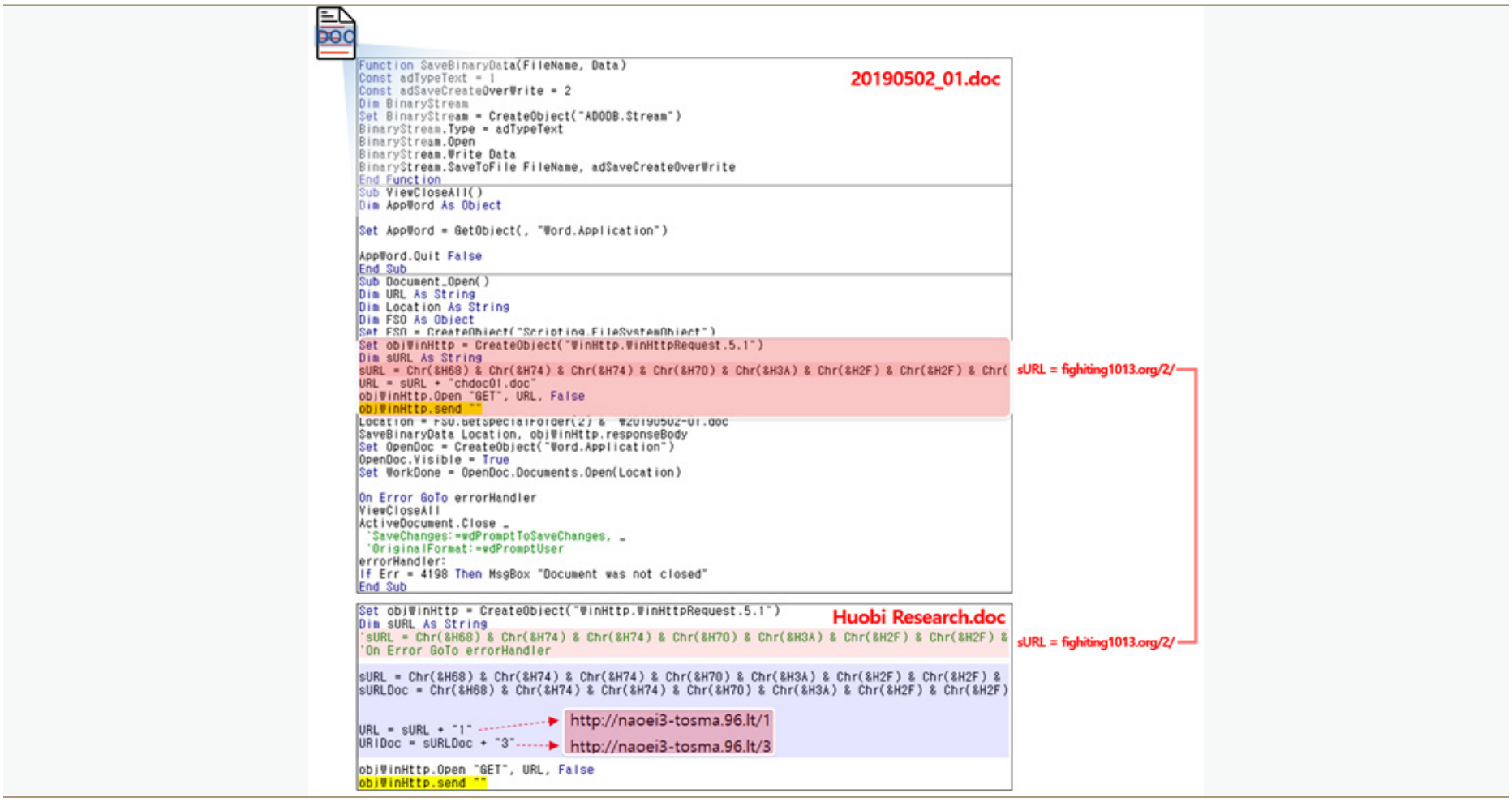
오퍼레이션 머니홀릭의 배후, 그들이 원하는 것은?

2018년 2월부터 2019년 8월까지 유포된 악성코드를 프로파일링한 결과, 오퍼레이션 머니홀릭이 수년간 국내 기관 및 기업에 대한 타깃 공격을 전개한 '김수키' 또는 '킴수키'로 불리는 Kimsuky 그룹과 관련된 정황을 포착했다.

우선, 2018년 2월에 발견된 감염 PC 중 한 곳에서 다수의 악성코드가 확인됐는데, 그 중에 Utilman.exe 파일이 포함되어 있었다. Utilman.exe 파일은 지난 2017년 2월에도 발견된 바 있으며, 당시 Utilman.exe 파일과 함께 발견된 키로거가 2013년 Kimsuky 그룹이 사용한 키로거와 동일하다. 또 Kimsuky 그룹이 2017년 8월부터 사용한 악성코드에 감염된 PC에서도 Utilman.exe와 유사한 기능을 가진 악성코드가 발견됐다.

또 다른 정황은 지난 2019년 5월 24일, 주요 백신 프로그램을 기반으로 악성코드 검사를 제공하는 바이러스토털(VirusTotal) 사이트에 Kimsuky 그룹이 유포한 파일('Huobi Research Weekly(Vol. 62) 2019.05.13-2019.05.19.

doc', 이하 Huobi Research.doc)에서 포착됐다. 오퍼레이션 머니홀릭 조직에서 사용한 C&C 서버 주소가 Huobi Research.doc 파일에도 동일하게 존재하나 주석처리 되어 있으며, 새로운 C&C 서버인 naoei3-tosma.96.lt가 추가됐다. 또 이들 파일의 등록정보를 확인한 결과, 만든 날짜(및 시간)와 만든 이도 동일한 것으로 나타났다.



[그림 9] 오퍼레이션 머니홀릭의 파일(위)과 Kimsuky 그룹의 파일(아래)의 악성 매크로 비교

이 밖에 다수의 관련성을 토대로 짐작할 수 있는 것은 지난 2월 안랩이 '오퍼레이션 카바 코브라 보고서'를 통해 언급한 바와 같이 Kimsuky 그룹을 비롯해 국내에서 타깃 공격을 전개하고 있는 공격자들이 금전적 이득 확대에 주력하고 있으며, 이에 따라 공격 범위가 더욱 확대될 가능성이 높다는 것이다.

오퍼레이션 머니홀릭에 관한 보다 상세한 내용은 ASEC이 발표한 'Operation Moneyholic: 금전적 이득을 목적으로 한 최신 표적 공격 사례' 보고서에서 확인할 수 있다.

▶'Operation Moneyholic' 분석보고서 전문 보기