월간 악성코드 분석 리포트 (2018-01)

가상화폐 채굴 악성코드 분석

수산INT 기술 연구소 (CERT)

2018. 01. 12

가상화폐 채굴 악성코드 관련 분석 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)

SOOSAN INT

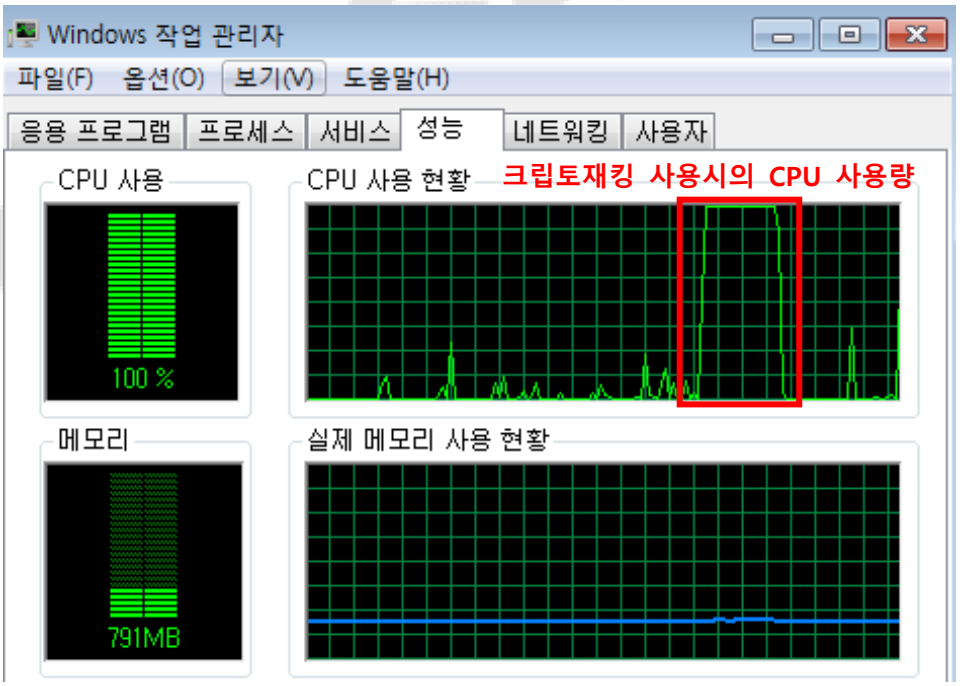
목 차

1. 개 요

2017년 최대 화두는 가상화폐입니다. 가상화폐 시세가 천정부지로 상승했기 때문으로 볼 수 있습니다. 2017년 1월 비트코인 시세는 100만 원 수준이었다면, 2017년 12월에는 2,000만 원을2,000만원을 돌파했습니다. 현재 하락세이긴 하나, 비트코인 시세는 여전히 높습니다. 12월 말 기준으로 1,600만 원 수준을 유지하고 있습니다. 이외에 여러 가상화폐의 시세가 올해 들어 급증했습니다.

이러한 추세는 가상화폐 취득을 목적으로 하는 악성코드 공격을 증가시킨 결과를 가져왔습니다. 그 중 대표적인 악성공격으로 '크립토재킹 (Cryptojacking)'이 있습니다. 크립토재킹 (CryptoJacking)은 개인 기기를 해킹해서 가상화폐 채굴에 악용하는 악성코드입니다.

크립토재킹은 가상화폐와 함께 최근 이슈화 되고 있는 악성코드 입니다. 이번 보고서에는 크립토재킹을 알아보도록 하겠습니다. 구성은 다음과 같습니다. 2장에서는 채굴과 크립토재킹의 일반적인 원리를 알아보도록 하겠습니다. 그리고 3장에서는 수산INT CERT팀에서 직접 분석한 내용을 소개하겠습니다.



2. 가상화폐 채굴 악성코드 (크립토재킹) 분석

2.1 가상화폐 채굴과 크립토재킹

국가 화폐는 중앙은행에서 발행된다면, 가상화폐는 채굴로 발행됩니다. 채굴은 문제를 맞힌 사용자에게 대가로 가상화폐를 지급하는 과정을 의미합니다. 대부분 가상화폐의 경우, 암호화된 문자열을 제시합니다. 그리고 이를 가장 먼저 해독한 사용자에게 가상화폐를 제공합니다. 아래의 프로세스는 비트코인의 채굴 과정을 정리한 것입니다.

1. "8a3a41b85b8b29ad444def299fee21793cd8b9e567eab02cd81" 암호값이 주어짐
2. 채굴자는 '무작위 대입법'으로 암호화 값을 해독함
3. 해독 대가로 채굴자는 비트코인을 얻음

암호화 값을 해독하기 위해서는 일일이 내용을 입력해보는 수밖에 없습니다. 결국은 내용을 빠르게 입력하는 사람이 가상화폐를 채굴하게 됩니다. 다시 말해, 가상화폐 채굴의 주요 핵심은 컴퓨터 성능에 달려 있습니다. 이러한 이유로, 여러 대 컴퓨터를 이용해서 채굴하는 경우가 늘어나고 있습니다. 참고로 채굴 위해서 컴퓨터를 모아 놓은 곳을 '마이닝 풀 (채굴 장)' 이라고 부릅니다. 컴퓨터가 많을수록 성능이 좋아지기 때문에, 가상화폐를 획득 할 확률이 그만큼 높아집니다.

중국의 비트메인은 수천 대의 컴퓨터를 이용해서 채굴 하고 있습니다. 하루 전기료만 4,400만 원입니다. 중국 물가를 고려하면 어마한 금액입니다. 또 다른 발전소의 경우, 전기료를 절감시기키 위해서 수력 발전소를 이용하는 경우도 있습니다[1]. 국내 강원도 홍천군에도 채굴장이 있는데, 2,000여 대의 컴퓨터가 있습니다[2]. 상황이 이렇다 보니 GPU 품귀 현상이 발생한 적도 있었습니다. 아울러 채굴장이 많아지다 보니, 가상화폐가 환경을

1) 중앙일보 (2017. 08. 31), "하루 전기료만 4400만원...비트코인 캐는 사람들", http://news.joins.com/article/21892530

2) 머니투데이 (2017. 10. 25), "가상화폐 채굴장 왜 강원도에? 현장 가보니", http://news.mt.co.kr/mtview.php?no=2017102515072025656

해친다는 말까지 나온 적이 있습니다.

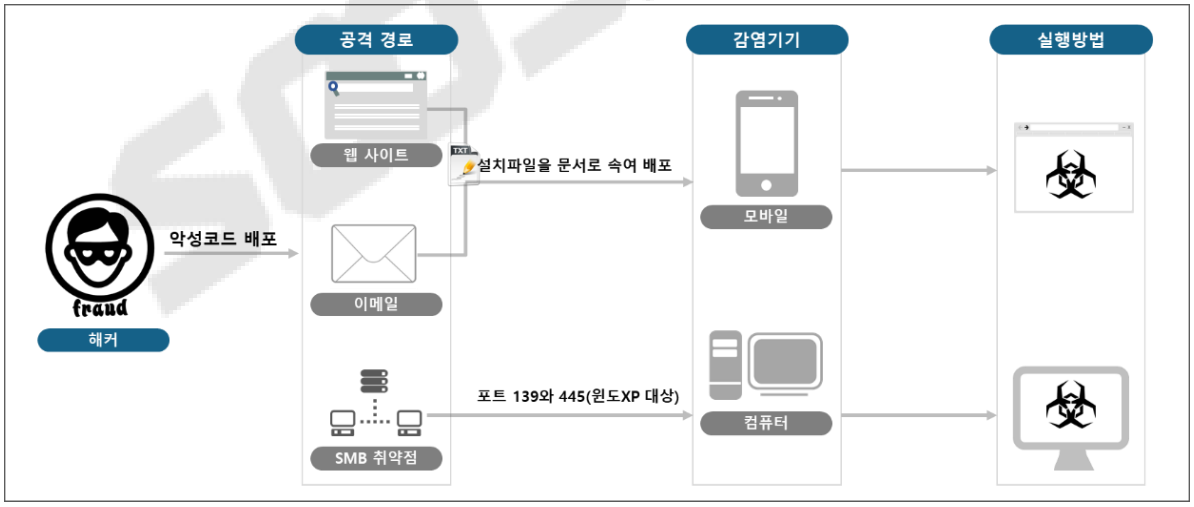
특히 비트코인의 경우 발행량이 2,100만 개로 한정돼 있습니다. 그래서 비트코인 채굴 경쟁은 매우 심각한 상황입니다. 더욱이 남은 비트코인 양은 얼마 되지 않습니다. 2017년 12월 24일 기준으로 비트코인 총 발행량의 80% (1,676만)가 이미 채굴되었습니다.

현재 가상화폐 시세는 하락하고 있습니다. 그런데도 가상화폐 시세는 여전히 높은 상황입니다. 이러한 추세가 반영되어, '크립토재킹'이라는 악성코드가 등장한 것입니다. 사실 크립토재킹은 가상화폐가 급상승 하는 시점인 2017년 6월에 쟁점화 되었습니다. 그러나 여전히 도처에 악성공격이 발생하고 있습니다[3].

해커는 크립토재킹으로 개인기기를 채굴 장비로 사용할 수 있습니다. 비용을 들이지 않고 남의 기기로 채굴을 할 수 있는 것입니다. 그럼 크립토재킹의 동작원리와 증상에 대해서 한번 알아보도록 하겠습니다.

2.2 크립토재킹 원리

크립토재킹 실행 원리는 아래와 같습니다.



3) Fortune (October 23, 2017), "Why Cryptojacking Is The Next Big Cybersecurity Threat", http://fortune.com/2017/10/23/bitcoin-monero-cryptocurrency-mining-security-threat/

2.2.1 공격경로

자체 연구에 따르면, 해커는 3가지 방법으로 크립토재킹을 전파하고 있습니다. 해커는 '워터링 홀' 수법을 이용해서 크립토재킹을 전파할 수 있습니다. 워터링 홀은 사이트에 악성코드를 심어서 방문자를 감염시키는 방법입니다. 크립토재킹의 성공 여부는 특정 대상 감염 여부가 아니라, 감염 사용자 수 입니다. 채굴 기기가 많아질수록 가상화폐 획득 성공률이 올라가기 때문입니다. 그래서 사용자 몰래 전파할 수 있기 때문에, 워터링 홀이 가장 적합하다고 볼 수 있습니다. 두번째 방법으로는 악성 이메일을 이용하는 것입니다. 문서 형태로 실행 파일을 속여서 크립토재킹 설치파일을 유포하는 것입니다. 사용자가 다운 후에 실행하면, 크립토재킹을 기기에 몰래 심게 됩니다. SMB (Server Messaging Block)를 이용해서 유포할 수도 있습니다. 참고로 SMB는 파일과 같은 공유를 목적으로 만들어진 통신 프로토콜이다 (포트는 139와 445를 사용한다). 한 마디로 제로데이와 같은 형태로 공격이 이뤄진다고 할 수 있습니다. 이더너블루는 마이크로소프트가 발표한 SMB 취약점을 업데이트하지 않은 기기를 찾는 툴인데, 취약 기기가 발견되면 더블펄사를 이용해서 기기에 크립토재킹을 은닉 시킵니다.

2.2.2 감염증상 (감염기기 및 행위)

감염 되는 기기는 주로 컴퓨터 입니다. 그러나 최근에는 컴퓨터 외에 모바일도 대상에 포함이 된다는 말이 있습니다. 아직은 이러한 사례가 발견되지 않았지만, 가상화폐 투자가 가열된다면 충분히 일어날 수 있는 일입니다. 실행방법은 두 가지로 나눌 수 있습니다. 우선 감염기기에 보이지 않는 폴더를 생성해서 채굴 악성코드를 심어서, 채굴에 이용하는 수법이 있습니다. 혹은 자바스크립트 기반 사이트에서 채굴 악성코드를 심어서 채굴에 이용하게 할 수도 있습니다. 보통 이러한 경우, 애드웨어 형태로 보이는 경우가 많습니다.

크립토재킹 원리를 살펴보았습니다. 크립토재킹을 사실 그렇게 사용자에게 위협적이지는 않습니다. 사용자 기기 성능에 영향만을 주기 때문입니다. 그렇다고 크립토재킹 위협을 안일하게 생각해서는 안 됩니다. 크립토재킹은 네트워크로 연결된 경우가 많은데, 해커가 크립토재킹 악성코드를 경로로 추가적인 악성코드를 심을 수 있기 때문입니다. 한마디로 악성코드 전파 창구로 이용할 수 있습니다.

3. 분석 사례 (ActivateDesktop)

수산INT CERT에서는 크립토재킹 악성코드를 수차례 분석해보았습니다. 대표적으로 하나의 사례만 들어서 크립토재킹 분석 사례를 소개하도록 하겠습니다.

3.1 분석 파일 정보

분석 파일명은 "ActiveDesktop.exe" 입니다. 해당 파일 해쉬 정보는 아래와 같습니다.

- MD5: 54b6b09962cbede423af9ac3f881117a
- SHA-1: 0004fabc375205237a74b86a94ef9bb3941b505a
- SHA-256: 07dd567986e5acbb4ff2e29099bf994ca2eaa726b3c4a59276628e39d3e54융

해당 파일에 C&C[4] 흔적이 발견되었는데요. "http:// 1.lalkaboy.z8.ru" 도메인이 해당 파일에서 확인됐습니다. 분석한 결과 공격자의 C&C 서버 주소였습니다. 아울러 드롭퍼[5] 역할을 하는 사이트인 "http:// http://1.lalkaboy.z8.ru/tools/RegWriter.exe.raum_encrypted"도 발견했습니다. 해당 파일을 실행하면, 아래 표와 같이 폴더와 파일이 추가 생성되었습니다.

구 분	생 성 명 (생성위치)
폴 더	.Trash-100 (C:₩)
	db (C:₩.Trash-100)
	version (C:₩.Trash-100₩유)
파 일 명	ActivateDesktop.exe (C:₩.Trash-100)
	framework_exe (C:₩.Trash-100₩db)

4) C&C (Command & Control): 원격으로 악성코드를 조종하는 기술을 말한다.

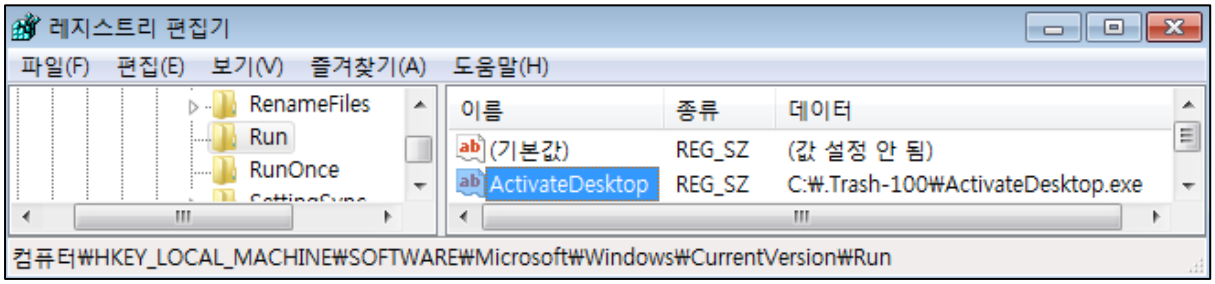
5) 드롭퍼 (Dropper): 악성코드를 설치 하는 역할을 맡은 애플리케이션 혹은 사이트를 말한다.

3.2 실행 증상

재부팅을 하여도 자동으로 실행할 수 있도록 레지스트리 추가

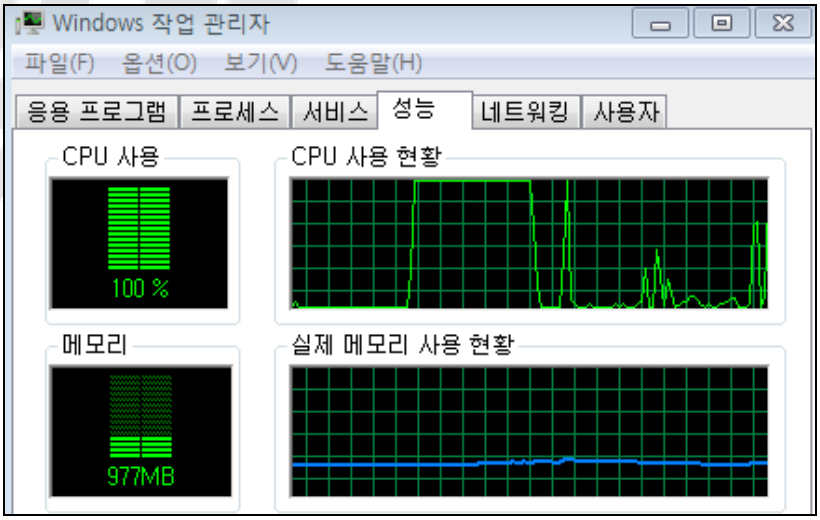
실행->regedit ->HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run

경로로 들어가서 ActivateDesktop 확인



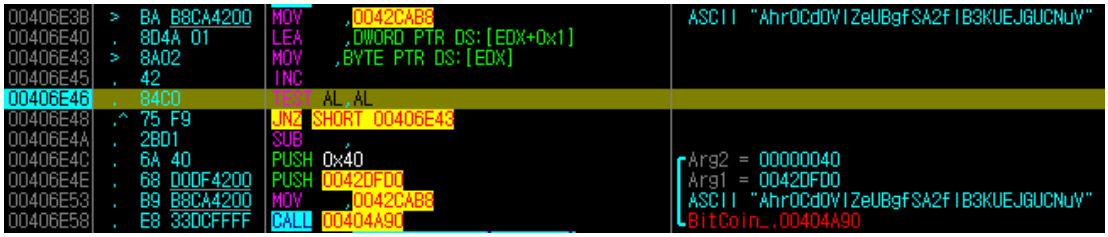
C:₩.Trash-100 숨김 폴더 생성

백그라운드(background)에서 실행되는 가상화폐 채굴 악성코드를 통하여 변동 되는 CPU 증상

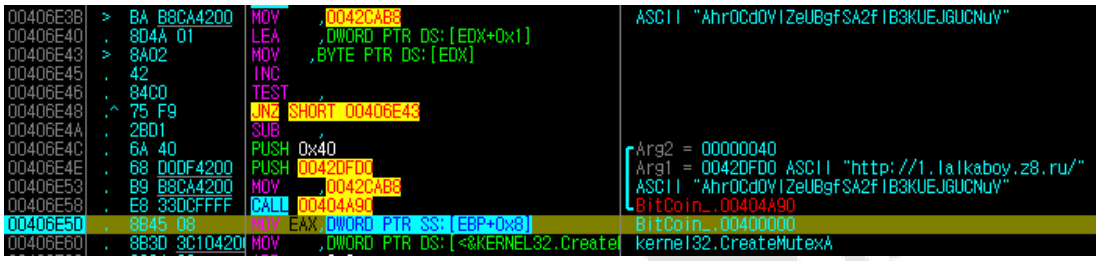


3.3 분석 내용 (크립토재킹 동작 프로세스 분석)

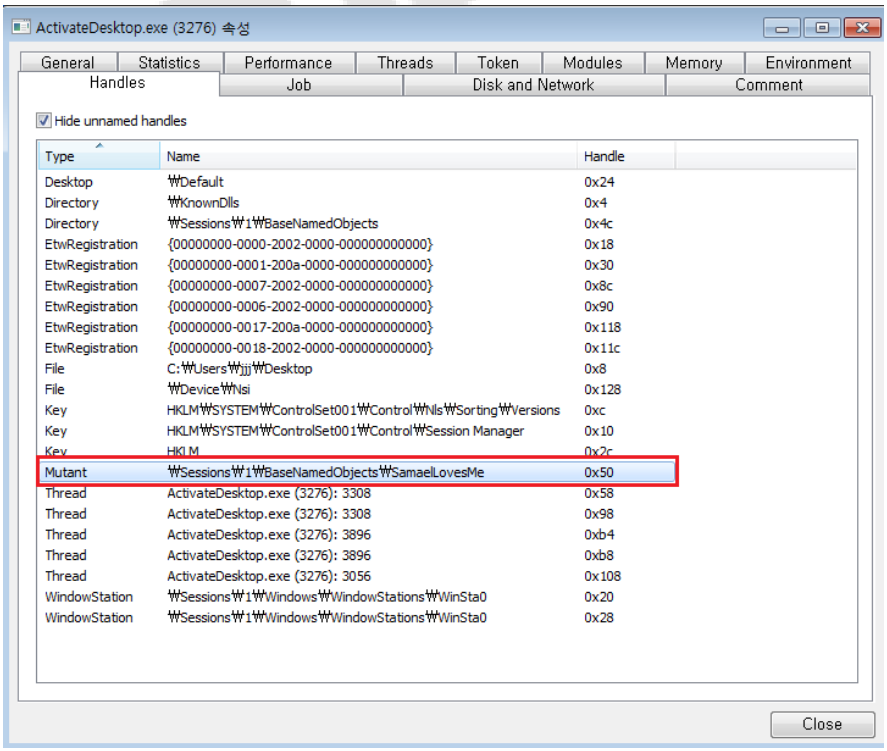
1. C&C 확인: "ru"라는 도메인을 사용했고, 난독화 되어 있었음



2. CALL 00404A90 호출 하여 난독화 해제하여 "http://1.lalkaboy.z8.ru/" 도메인 발견

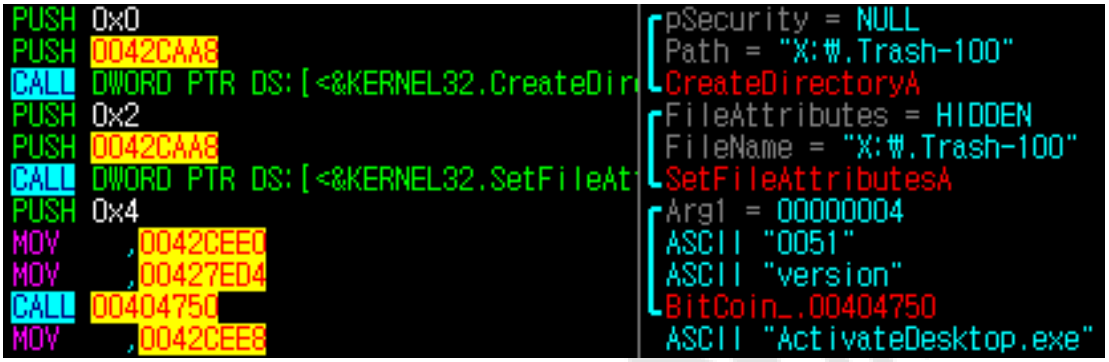


3. "SamaelLovesMe" 것이 발견됨. 이 파일은 중복 실행을 확인하는 파일 임

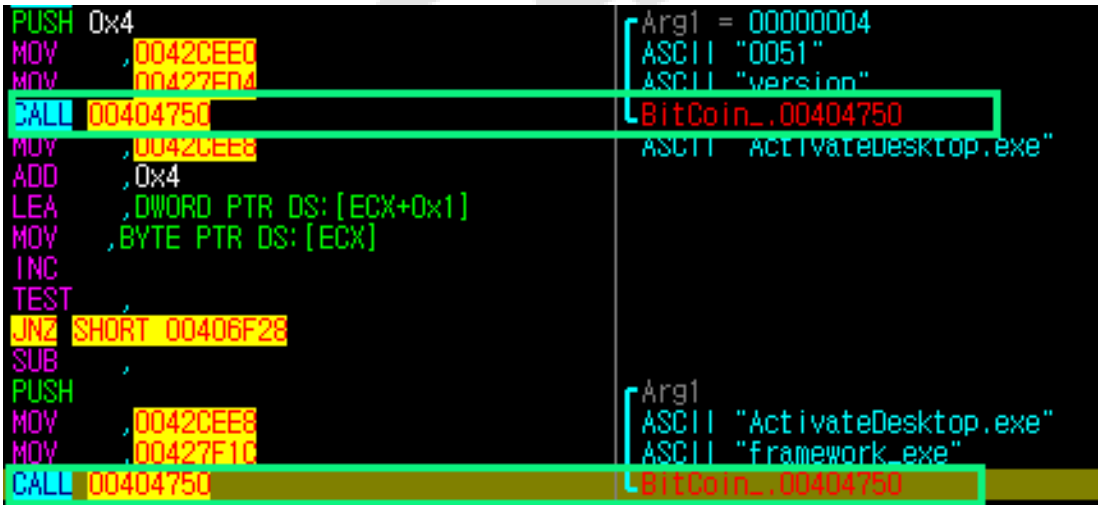


4. 00408000 주소의 함수를 CALL 하여 FirewallGUI.exe 파일 실행되었는지 확인해서 FirewallGUI.exe 란 파일이 실행되어 있으면 실행 중인 해당 프로세스 종료함.

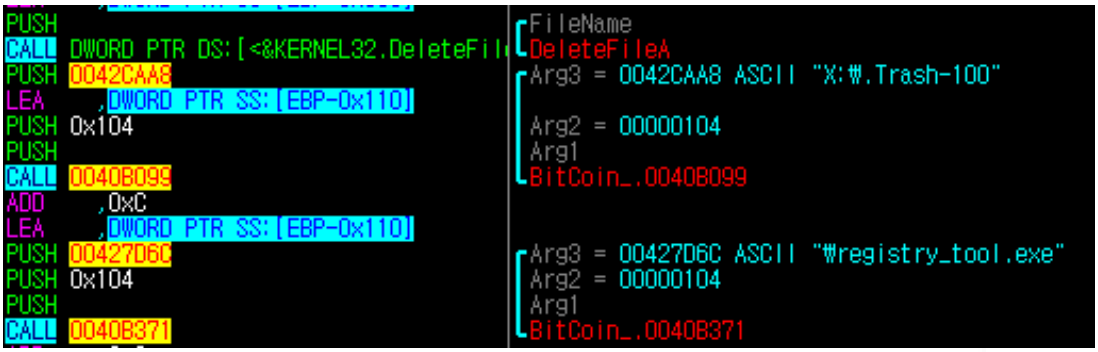
5. FirewallGUI 파일이 실행되어 있지 않다면 CreateDirectoryA 함수를 사용해 "C:₩.Trash-100" 숨김폴더를 생성



6. "C:₩.Trash-100" 폴더 생성 후 "db" 폴더를 추가 생성하여 framework_exe, version 파일을 생성하여 파일 안의 내용을 추가



7. ASCII에서 생성할 파일 이름과 파일 안의 추가할 내용이 담겨 있음. 그리고 CALL 00404750의 주소는 위의 ASCII 정보를 Stack에 담고 파일 생성과 내용을 추가함. ActivateDesktop.exe 파일을 레지스트리에 등록하여 재부팅 하여 자동 실행이 되게끔 하는 채굴 행위를 최종적으로 발견함



3.4 대응 방안

크립토재킹 감염 예방을 위해서는 어떻게 해야 할까요? 방법은 3가지 입니다.

1. **eWalker 설치로 악성사이트 접속 차단.** 악성 사이트에 접속을 하지 않는 것이 가장 중요한 예방법 입니다. 그런데 문제는 악성 사이트를 탐지하는 것은 쉽지 않습니다. 자사에서 제공하는 **eWalker 제품은 40만개가 넘는 악성URL을 보유하고 있습니다. 이를 활용하면, 쉽게 워터링 홀로 인한 감염을 예방할 수 있습니다. ActiveDesktop.exe의 C&C 도메인의 경우, eWalker에서 이미 차단하고 있습니다.**

C&C 서버 (도메인 & IP)	
1	http:// 1.lalkaboy.z8.ru (80.93.62.207)
2	http:// http://1.lalkaboy.z8.ru/tools/RegWriter.exe.raum_encrypted

2. 운영체제 업데이트도 중요합니다. SMB는 운영체제의 취약점을 이용한 공격이기 때문에, 항시 업데이트를 해야 합니다.
3. 의심되는 메일을 열지 않는 것도 중요한 예방법입니다. 출처를 알 수 없는 메일에는 악성코드를 숨겨놓을 가능성이 높기 때문입니다.

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