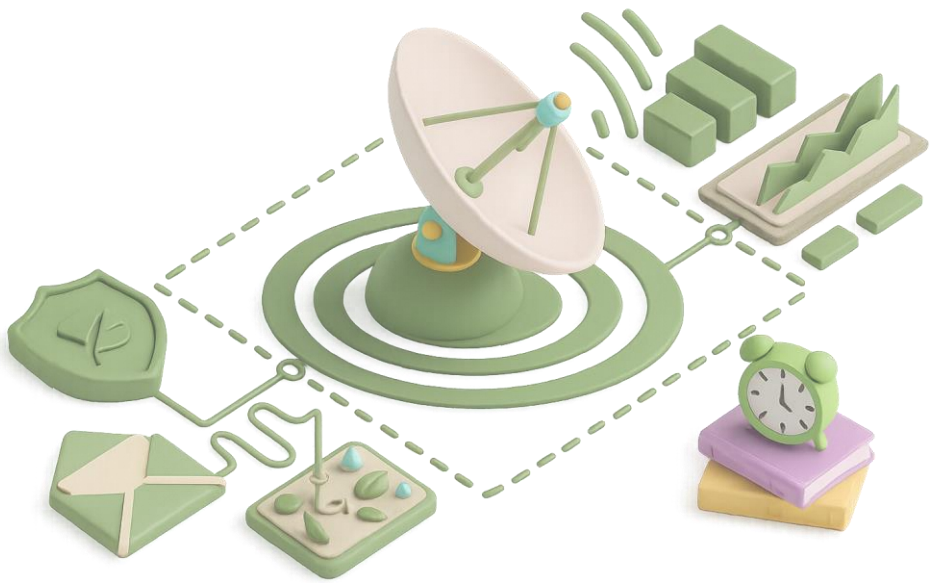
SGA 보안레이더

보안위협 리포트

Vol. 12
2026.05

5월의 악성코드 분석

LockBit 5.0 랜섬웨어



SGA 에스지에이솔루션즈(주)

SGA보안레이더 발행본 다운로드

썸네일을 클릭하시면 앞서 발행된 SGA보안레이더를 다운받으실 수 있습니다.

▶2025년

2025.07
주요이슈
SwaetRAT

2025.08
주요이슈
링크파일 활용한 백도어 악성코드

2025.09
주요이슈
Gunra Ransomware

2025.10
주요이슈
LockBit 4.0 랜섬웨어

2025.11
주요이슈
RokRAT

2025.12
주요이슈
HybridPetya

▶2026년

2026.01
주요이슈
DarkCloud Stealer

2026.02
주요이슈
문서위장 악성파일

2026.03
주요이슈
와이퍼(Wiper) 악성코드

2026.04
주요이슈
LiteLLM 악성코드

CONTENTS

발행일자: 2026년 5월

1. 2026년 4월 보안 동향

2026년 4월 사이버 공격이 많이 발생한 것으로 확인되었다.

검색 수익화 기업을 표방하여 최상위 권한을 획득하고 백신 무력화

검색 수익화 기업을 표방한 드래곤보스솔루션(Dragon Boss Solutions)의 소프트웨어가 정상적인 업데이트 경로를 악용해 운영체제의 최상위 권한을 장악하고 백신 제거 스크립트를 배포를 하였다.

해외 보안 기업인 헌트리스(Huntress)의 연구진은 'RaceCarTwo.exe'이라는 실행 파일을 통해 시작되는 감염 경로를 추적하였으며, 이 공격을 포착한 것으로 확인된다.

공격에 사용된 'ClockRemoval.ps1'이라는 스크립트는 백신 프로세스를 강제 종료할 뿐만 아니라 레지스트리를 조작하여 보안 서비스 자체를 삭제하고, 윈도우의 호스트 파일을 수정해 멀웨어바이트나 카스퍼스키 등의 백신 업데이트 경로를 차단하여 재설치가 불가능하도록 조작하는 것으로 확인된다.

이번 공격으로 25,000개 이상의 시스템이 위험에 노출되었으며, 실제 감염 IP는 23,565개인 것으로 확인된다.

#해킹그룹 TeamPCP 공식 도커 허브 저장소에 가짜 이미지 주입하여 공급망 공격

해킹 그룹인 팀PCP(TeamPCP)가 공식 도커 허브 저장소인 'checkmarx/kics'에 악성코드가 삽입된 가짜 이미지를 주입하여 공급망 공격을 한 것으로 나타났다.

해외 기업인 JFrog와 Socket이 발표한 보고서에 따르면 오염된 바이너리는 인프라 코드 스캔 보고서를 암호화해 외부로 빼돌리는 정보 탈취 기능을 실행하는 것으로 확인된다.

공격자들은 도커 이미지를 넘어 비주얼 스튜디오 코드 확장 프로그램에도 악성코드가 삽입된 패키지를 업로드한 것으로 확인된다. 이 악성코드는 깃허브 토큰과 노드 패키지 매니저 자격 증명을 비롯한 아마존 웹 서비스, MS의 Azure 등 개발 환경에 저장된 모든 정보를 탈취하는 것으로 확인된다.

탈취한 정보는 자신들이 관리하는 텔레메트리(Telemetry) 엔드포인트인 'audit.checkmarx.cx'로 전송해 추적을 따돌리며, 탈취한 토큰을 악용해 피해자 계정에 가짜 저장소를 몰래 생성해 업로드한 것으로 확인된다. 또한 훔친 npm 자격 증명을 이용해 피해자가 관리하는 정상 패키지를 악성 버전으로 다시 배포하는 것으로 확인된다.

2. 악성코드 통계 및 분석

2026년 4월 한 달 동안 사용자 PC에서 **탐지된 악성코드는 총 99,331건으로 확인**되었으며, 지난 3월과 비교하여 94%의 높은 증가율을 기록했다.

가장 많이 탐지된 악성코드 유형은 Trojan이었으며, Virus, Exploit 형태의 악성코드 유형이 차지하였다. 3월과 비교하면 Trojan.GenericKD, Win32.Virtob에 대한 탐지 비율이 증가하였다.

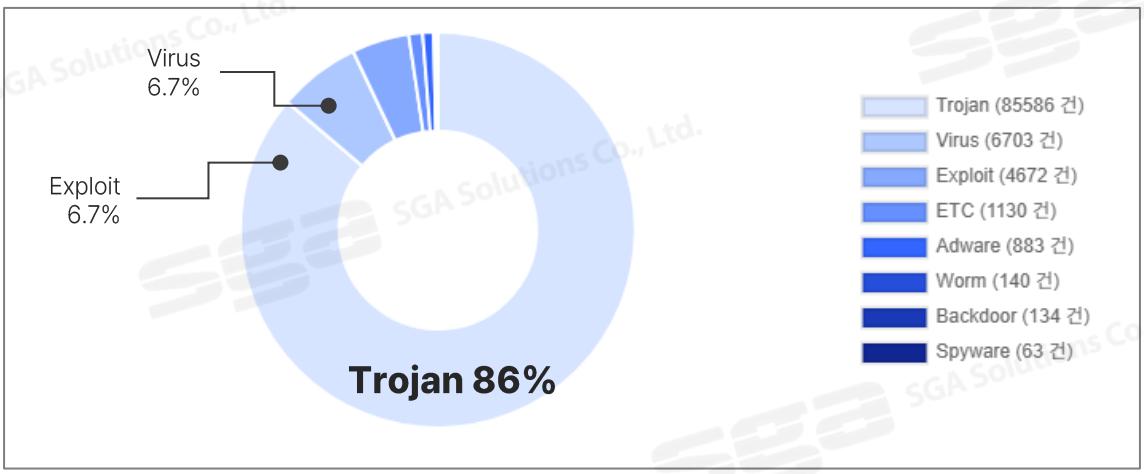
수집된 피싱 메일은 204건 이었으며, 3월에 이어 4월에도 '업무/계약 문서 확인'이 사용자를 속이기 위해 가장 많이 사용된 메일 본문으로 기록되었다. 가장 많이 수집된 피싱 메일 공격 유형은 악성 URL이 첨부된 하이퍼링크 형태의 피싱 메일이었다.

■ 유형별 탐지 통계

4월 한 달 동안 사용자 PC에서 탐지된 악성코드의 유형을 확인한 결과 **Trojan 형태의 악성코드가 85,586건(86%)으로 1위를 차지**했으며, Trojan 형태의 악성코드 중 Ransomware의 탐지 비율이 여전히 높았으며, Generic도 꾸준히 탐지 되고 있다.

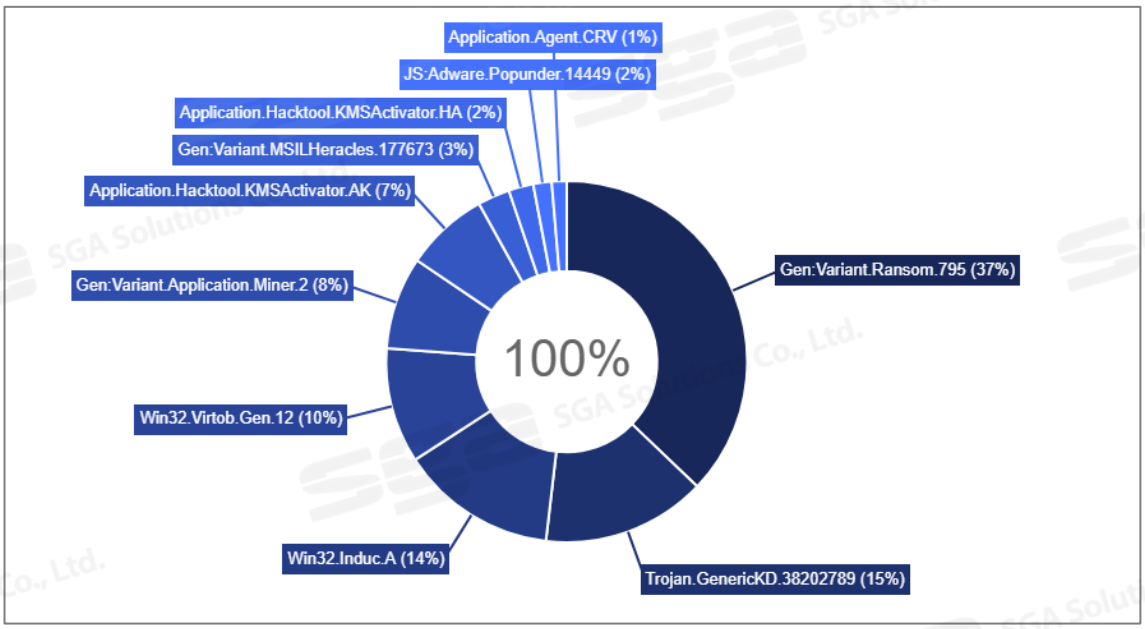
그 다음으로 컴퓨터의 소프트웨어나 하드웨어 관련 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격하는 **Exploit 형태의 악성코드가 6,703건(6.7%)으로 2위**를 차지했다. 3월에는 탐지 되지 않았던 Win32.Virtob가 탐지가 되었다.

마지막으로 자기 스스로는 행동할 수 없고, 정상 프로그램에 기생하여 실행되는 **Virus 형태의 악성코드가 4,672건(4.7%)으로 3위를 차지**했다.



[2026년 4월 유형별 탐지 통계]

■ 악성코드 TOP 10 탐지 통계

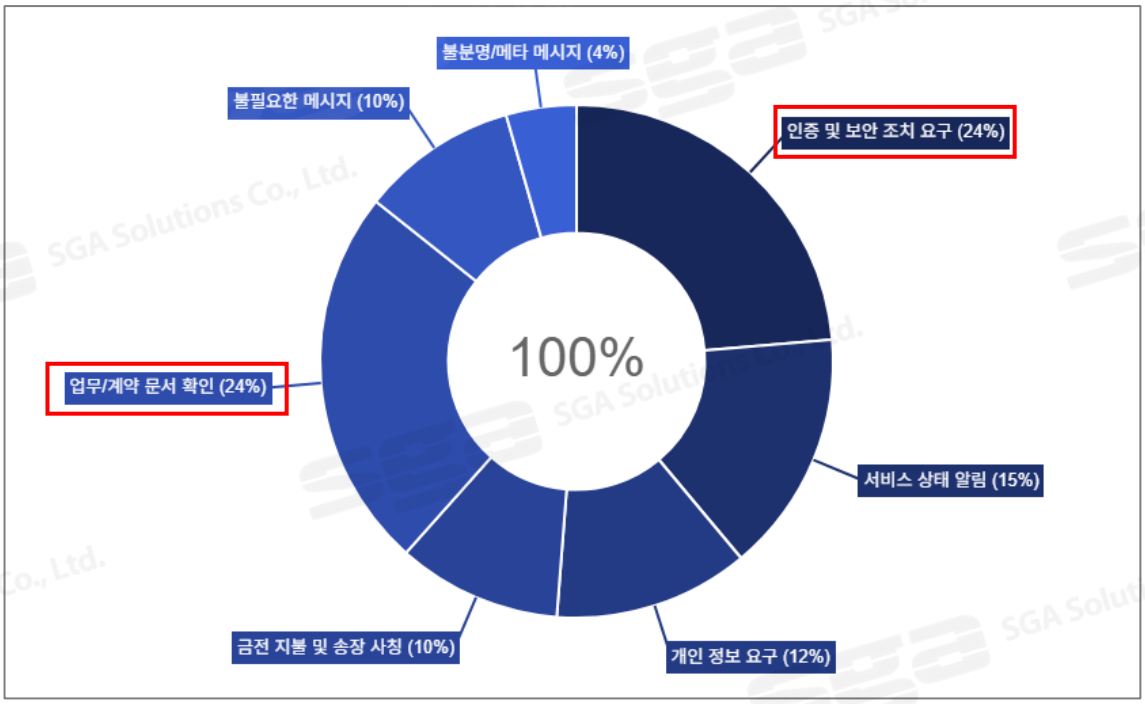


[2026년 4월 악성코드 TOP 10 탐지 통계]

2026년 4월 한 달 동안 사용자 PC에서 많이 탐지된 악성코드 중 가장 많이 탐지된 악성코드는 **사용자 PC의 파일을 암호화하여 사용자가 사용할 수 없게 만들며 암호화를 풀어주는 조건으로 금전을 요구하는 악성 소프트웨어의 진단명인 Ransom.795가 차지했다.**

그 다음으로 사용자가 알지 못하게 악성코드가 정상적인 프로그램으로 위장하는 악성코드와 유사한 동작을 하는 진단명인 Trojan.GenericKD가 3위에는 델파이의 특정 라이브러리가 감염된 후 컴파일 과정에서 생성되는 EXE 및 DLL 등에 바이러스 코드가 삽입되어 악성 행위를 하는 악성코드 진단명인 Win32.Induc.A가 올랐다.

■ 피싱 메일 본문 및 공격 유형 통계



[2026년 4월 악성코드 피싱 메일 본문 유형 통계]

2026년 4월 한 달 동안 **수집된 피싱 메일은 204건**이었으며, 그 가운데 "업무/계약 문서 확인" 내용이 담긴 피싱 메일이 49건(24%)으로 가장 많았다. 견적서 관련 내용이 담긴 문서 열람을 유도하는 메일이 가장 많았으며, 그 외에 업무 관련 내용이 담긴 계약서가 많았다.

그 다음으로 **"인증 및 보안 조치 요구" 내용을 담은 피싱 메일이 48건(24%) 수집**되었다. 비밀번호 만료가 되어 비밀번호 변경에 대한 내용이 담긴 메일이 많았으며, 그 외에 인증 요구, 보안 정보 업데이트에 대한 내용이 뒤를 이었다.

첨부 파일이 포함된 피싱 메일은 40건이 수집되었으며, 첨부 파일의 종류는 PE 파일 3건, Script 파일 22건, 그 외 15건이 수집되었다.

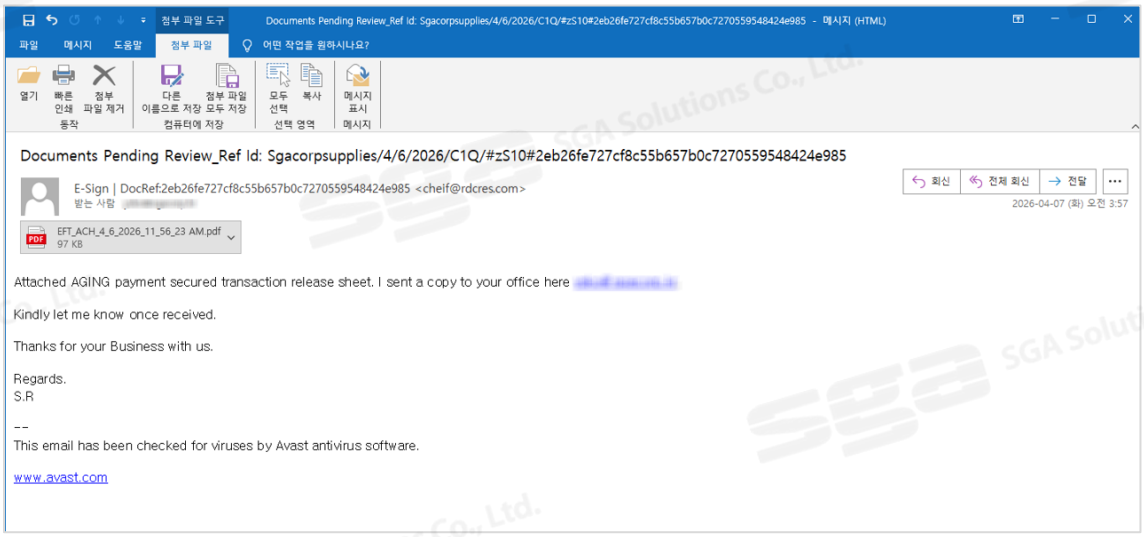
수집된 악성코드 중 대부분이 Script와 문서 파일을 이용해 사용자를 속이는 형태의 악성코드였으며, 최종적으로는 특정 영역을 클릭하도록 유도하는 형태로 확인된다.

이러한 악성코드에는 로그인을 유도하기 위한 악성 도메인 또는 추가 악성 행위를 위해 다운로드하는 URL이 담겨 있어 사용자의 주의가 필요하다.

3. 피싱 메일 분석

수집된 메일 중 인증 및 보안 조치 요구한 피싱 메일에 대해 분석을 진행하였으며 분석 내용은 다음과 같다.

- 메일 확인



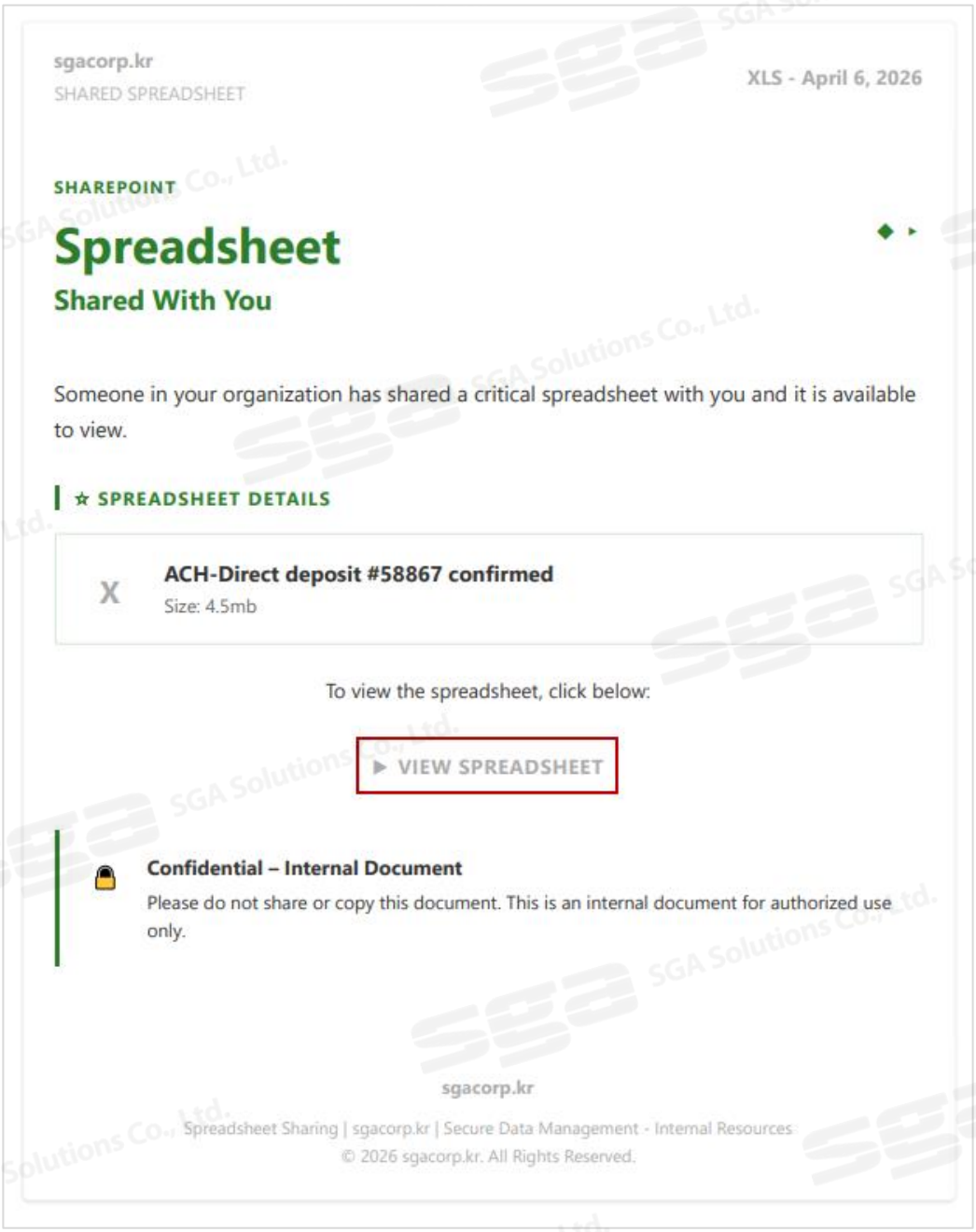
[메일 본문]

메일 본문은 "첨부된 AGING 결제 담보 거래 해제 명세서를 보내 드렸습니다"라는 문구로 시작하며, 수신자가 첨부 파일을 자연스럽게 열어보도록 유도한다.

메일 본문 마지막에 "이 이메일은 Avast 바이러스 백신 소프트웨어로 바이러스 검사를 완료했습니다" 문구와 함께 Avast 공식 사이트 링크 "www.avast.com"가 삽입되어 있다.

이는 수신자에게 해당 메일이 안전하다는 인식을 심어 첨부 파일 실행에 대한 경계심을 낮추려는 목적으로 활용된다.

- 첨부파일: EFT_ACH_4_6_2026_11_56_23 AM.pdf



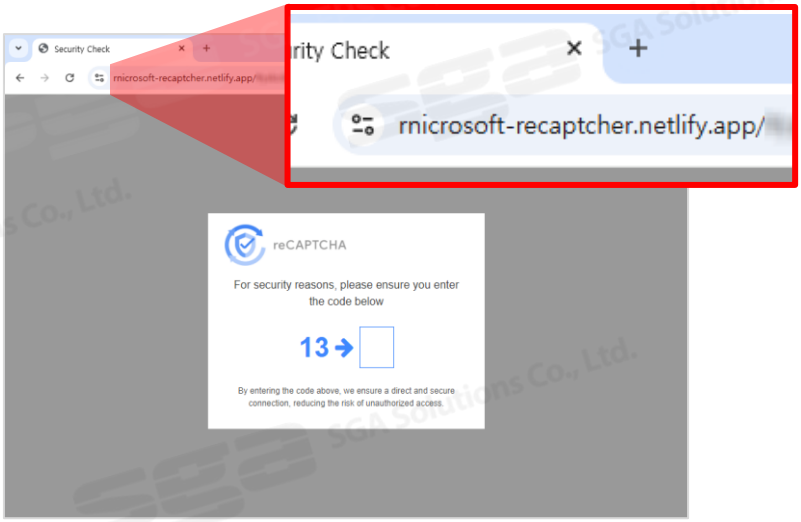
[Microsoft SharePoint로 위장한 첨부파일]

첨부된 PDF 파일은 Microsoft SharePoint의 스프레드시트 공유 알림 페이지로 위장하고 있다.

"VIEW SPREADSHEET"버튼에는 URL 주소를 짧게 줄여주는 단축 서비스 rb.gy를 활용한 단축 URL이 삽입되어 있으며, 이를 통해 실제 악성 도메인을 은닉하고 있다.

해당 링크의 실제 연결 주소는 “hxxps[:]//rnicrosoft-recaptcher.netlify.app”으로 클릭 시 캡차 페이지로 연결된다

- 캡차 페이지

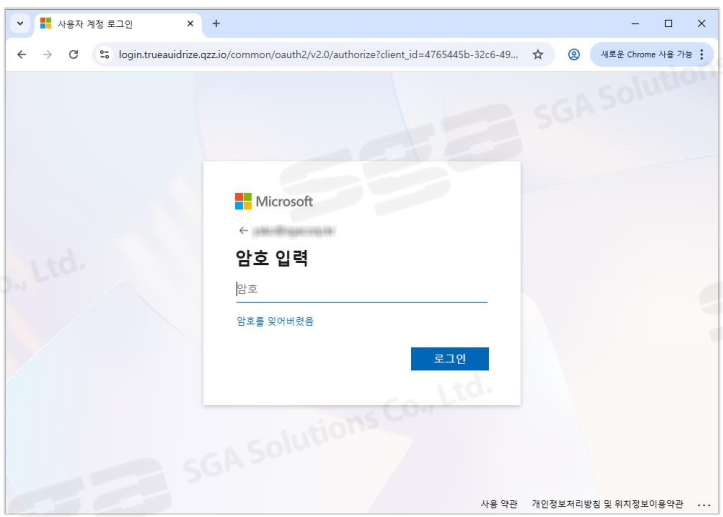


[캡차 페이지]

해당 캡차 페이지는 **소문자 'rn'을 이용해 'm'으로 보이도록 하여 Microsoft를 사칭하는 도메인**을 사용한다.

캡차 통과 시 중간 경유 서버 “hxxps[:]//trueauidrize.jacmaddox88.workers.dev”를 거쳐 최종 자격 증명 탈취 페이지로 리다이렉션된다.

- 자격증명 탈취 페이지

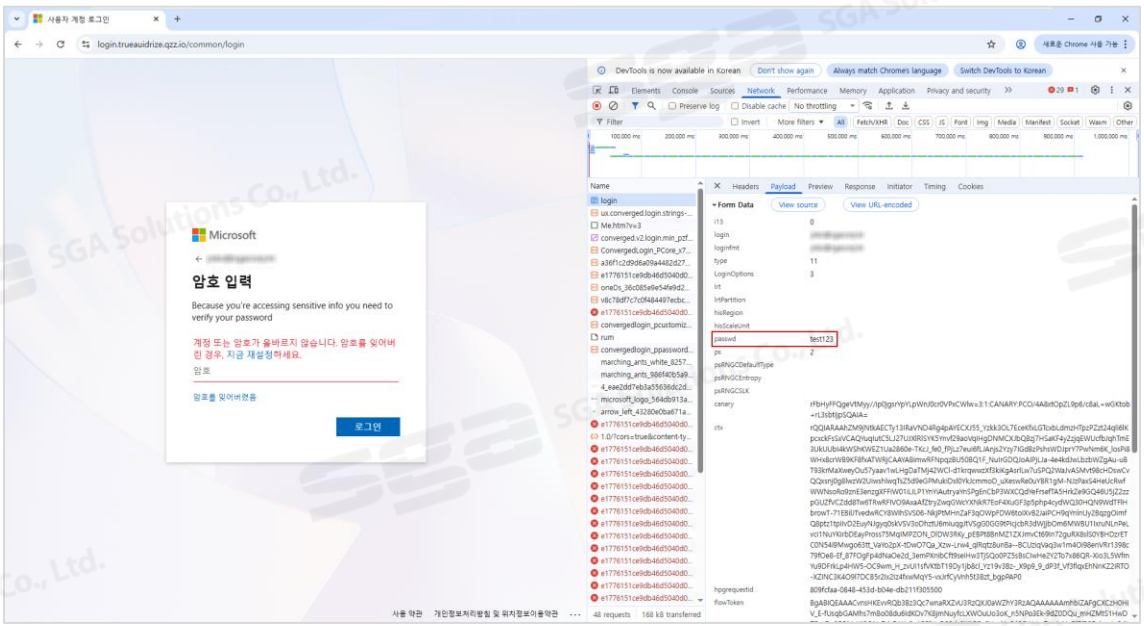


[Microsoft 사칭 페이지]

Microsoft 도메인과는 다르지만 Microsoft 로그인 페이지를 모방하여 정상 페이지와 구분하기 어렵도록 제작되어 있다.

이전 단계에서 전달된 피싱 메일 수신자의 이메일 주소가 자동으로 입력된 상태로 표시되며 수신자에게 암호 입력을 유도하고 있다.

- 정보 탈취 C2



[정보 탈취]

사용자가 자격 증명 탈취 페이지에서 암호를 입력하고 로그인 버튼을 클릭할 경우 암호가 올바르지 않다는 문구가 표시된다.

입력된 자격 증명은 POST 방식으로 C2 서버 “hxxps[:]//login.trueauidrize.qzz.io/common/login”로 전송되는 것으로 확인된다.

전송 데이터에는 피싱 메일 수신자의 이메일 계정 및 입력된 암호가 포함되어 있다.

4. 악성코드 분석

LockBit 5.0 버전의 악성코드가 수집되어 분석을 진행하였다.
자세한 분석 내용은 다음과 같다.

■ 개요

해킹 그룹인 LockBit은 2019년부터 랜섬웨어 서비스(RaaS:Ransomware-as-a-Service) 형태로 운영되는 사이버 범죄 그룹으로 알려져 있다.

2024년에 LockBit은 국제 공조 수사 크로노스 작전(Operation Cronos)으로 인프라가 무력화되었으나 2025년 2월에 LockBit 4.0 랜섬웨어가 그린과 블랙 버전 두 가지를 출시하여 자신들의 건재함을 과시했다.

이후 해외 보안 분석가인 'ChuongDong'이 2025년 3월 15일에 LockBit 4.0 버전을 상세하게 분석한 게시글을 게시하였으며, 9월에 LockBit 5.0이 모습을 드러냈다.

LockBit 5.0 랜섬웨어는 구조적으로 로더와 랜섬웨어 두 가지로 나누어져 있으며, 랜섬 노트에 ChuongDong 버전으로 명시되어 있는 것으로 확인된다.

이 랜섬웨어의 실행은 로더가 정상 파일을 이용하여 자식 프로세스를 생성한 후에 프로세스 할로잉(Process Hollowing) 기법을 통해 랜섬웨어를 주입하여 실행한다.

본 분석은 LockBit 4.0과 5.0의 차이점 중심으로 기술한다.

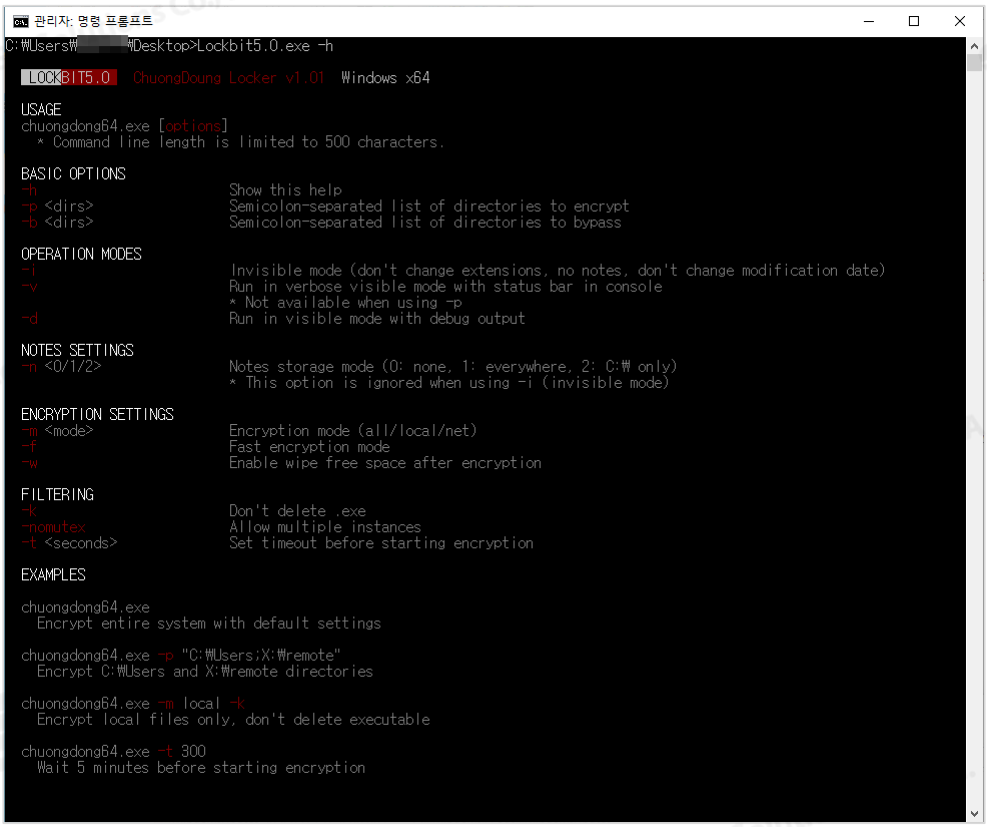
■ 주요 기능

- 사용자 관련 TEMP 폴더 내부 삭제
- 윈도우 이벤트 추적(ETW) 비활성화
- 복구 무력화
- 파일 암호화
- 윈도우 보안 로그 삭제
- 디스크 포렌식 무력화
- 금전 요구

■ 상세 분석

LockBit 로더 분석

- 명령어 도움말



[-h 입력 시 명령어 도움말 출력]

로더 파일은 Blender.exe 파일명으로 되어 있으며, 해당 파일명과 전혀 상관없는 자동차 부품 제조사 관련 디지털 서명 "BorgWarner"을 사용한 것으로 확인된다.

이 인증서는 불법으로 획득하였거나 탈취된 인증서로 판단되며, 정상 소프트웨어로 위장하여 보안 솔루션의 탐지를 우회하려는 시도로 확인된다.

로더 파일은 별도의 명령어 옵션 없이 단독으로 실행이 가능하며, "-h" 옵션을 통해 사용 가능한 명령어들을 확인할 수 있다.

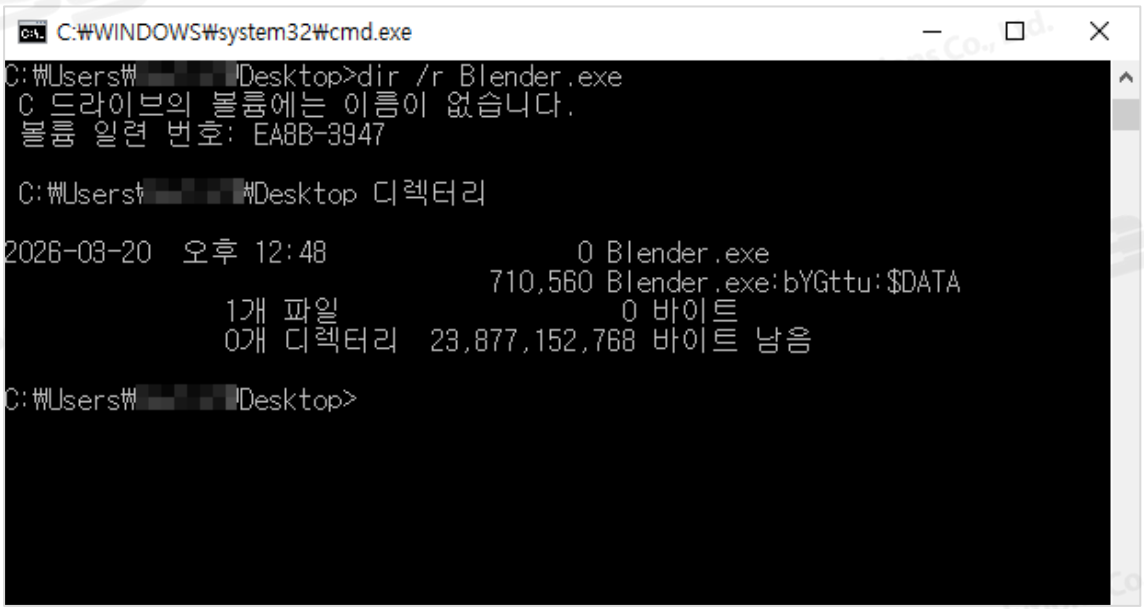
로더를 실행하면 먼저 안티 디버깅에 사용되는 CheckRemoteDebuggerPresent과 IsDebuggerPresent API를 사용하여 디버깅 여부를 확인한 후에 기능을 실행한다.

또한 NtClose API를 주기적으로 호출하여 유효하지 않은 핸들 처리로 인한 에러 처리 흐름을 이용한 안티 디버깅 방법도 적용되어 있다.

"-h"를 이용하여 확인할 수 있는 명령어 영문을 해석하면 다음과 같다.

카테고리	명령 매개변수	기능 설명(번역)
기본 옵션(BASIC OPTIONS)	-h	도움말 표시
기본 옵션(BASIC OPTIONS)	-p <dirs>	암호화할 디렉터리 목록 지정(세미콜론으로 구분)
기본 옵션(BASIC OPTIONS)	-b <dirs>	암호화에서 제외할 디렉터리 목록 지정(세미콜론으로 구분)
작동 모드(OPERATION MODES)	-i	숨김 모드 (파일 확장자 변경 안 함, 랜섬 노트 생성 안 함, 파일 수정 날짜 유지)
작동 모드(OPERATION MODES)	-v	콘솔에 상태 표시줄을 보여주는 상세 표시 모드로 실행 -p 옵션과 함께 사용 불가
작동 모드(OPERATION MODES)	-d	디버그 로그 출력을 표시하는 모드로 실행
랜섬 노트 설정(NOTES SETTINGS)	-n <0/1/2>	랜섬 노트 저장 모드 (0: 생성 안 함, 1: 모든 곳에 생성, 2: C:\ 드라이브에만 생성) -i (숨김 모드) 사용 시 이 옵션은 무시됨
암호화 설정(ENCRYPTION SETTINGS)	-m <mode>	암호화 대상 범위 모드 지정 (all: 전체 / local: 로컬 드라이브 / net: 네트워크 공유)
암호화 설정(ENCRYPTION SETTINGS)	-f	빠른 암호화 모드
암호화 설정(ENCRYPTION SETTINGS)	-w	암호화 완료 후 디스크 빈 공간 완전 삭제(Wipe) 기능 활성화
필터링 및 기타(FILTERING)	-k	랜섬웨어 실행 파일(.exe) 자가 삭제 방지
필터링 및 기타(FILTERING)	-nomutex	뮤텍스 검사를 우회하여 여러 개의 프로세스 다중 실행 허용
필터링 및 기타(FILTERING)	-t <seconds>	암호화 작업을 시작하기 전 대기할 시간(초 단위) 설정

- 자가 삭제



[파일 삭제 대기 중 정보 확인]

윈도우 운영 체제에서 열려 있는 파일 핸들을 사용하여 파일의 다양한 속성이나 정보를 변경하는 Native API인 ZwSetInformationFile을 두 번 사용하여 자기 자신을 삭제한다.

첫 번째 사용은 대체 데이터 스트림(Alternate Data Stream/ADS)으로 변경하여 원래 있던 파일은 크기가 0이 되며, 이때 이름에 콜론(:)과 랜덤 6글자(예: bYGttu)로 추가되고 비가시화 상태가 된다.

두 번째 사용은 삭제 플래그를 사용하여 삭제 대기 상태로 전환시키는 것으로 사용되며, 이후 파일의 핸들이 해제되는 시점에 운영 체제에 의해 삭제가 완료된다.

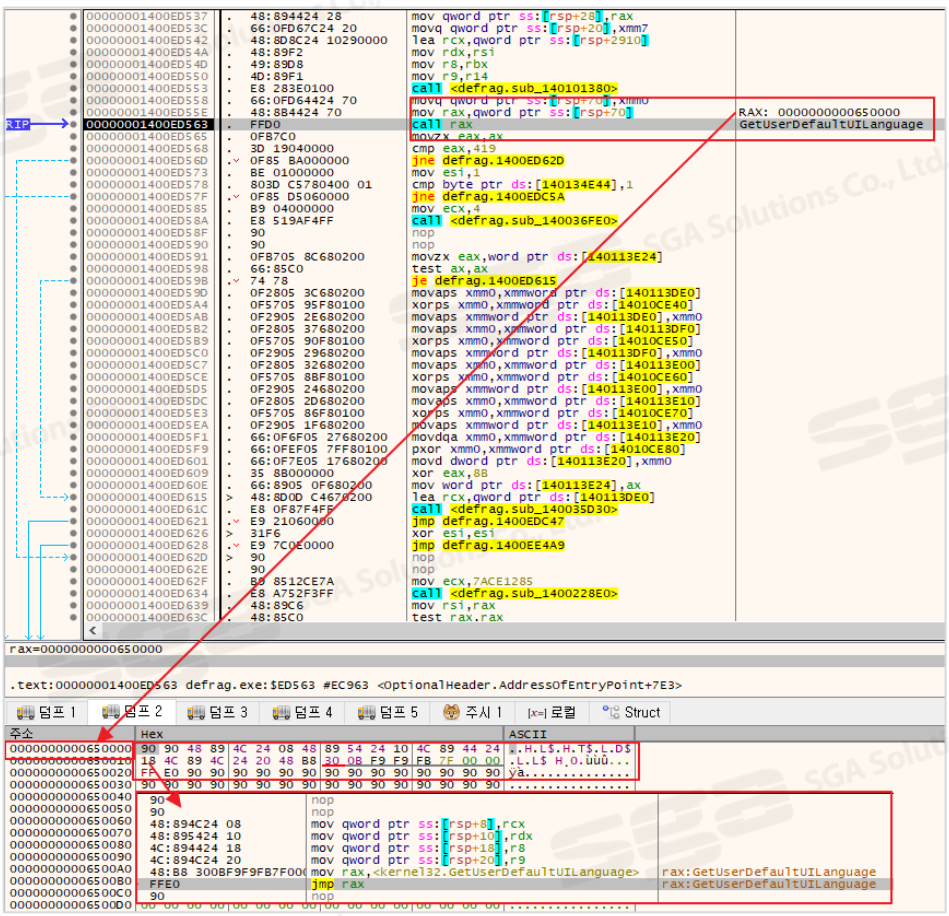
이와 같은 방식으로 삭제하는 이유는 프로세스에 파일이 매핑된 상태임에도 불구하고 앞서 언급한 ADS를 이용하면 운영체제가 삭제 플래그 설정을 허용하게 할 수 있기 때문이다.

로더가 자가 삭제를 완료한 후 페이로드의 랜섬웨어 동작은 자식 프로세스로 생성된 defrag.exe을 프로세스 할로잉 기법을 통해 주입하여 실행한다.

이때 사용되는 defrag.exe은 윈도우의 디스크 조각 모음 유틸리티로 사용되며, 정상 프로세스로 위장을 통해 악성 행위를 은닉하는 것이 목적이다.

LockBit 5.0 - ChoungDong Version

- 실행 환경 확인 및 API 해싱 - 실시간 호출



[실행 환경 확인 기능]

사용할 API를 노출 방지를 위해 커스텀 해시 알고리즘이 적용되었으며, 런타임에 API 주소를 계산하는 동적 API 리졸빙(Dynamic API Resolution)을 사용한다.

힙에 트램폴린 스텁(Trampoline Stub)이 생성되고 CALL로 할당된 스텁 주소로 진입한 뒤 JMP 명령을 통해 실제 API 주소로 간접 호출하는 방식으로 동작한다.

랜섬웨어의 암호화 대상에서 제외할 언어 및 지역을 확인하기 위해 GetUserDefaultUILanguage와 GetUserGeoID API를 사용한다.

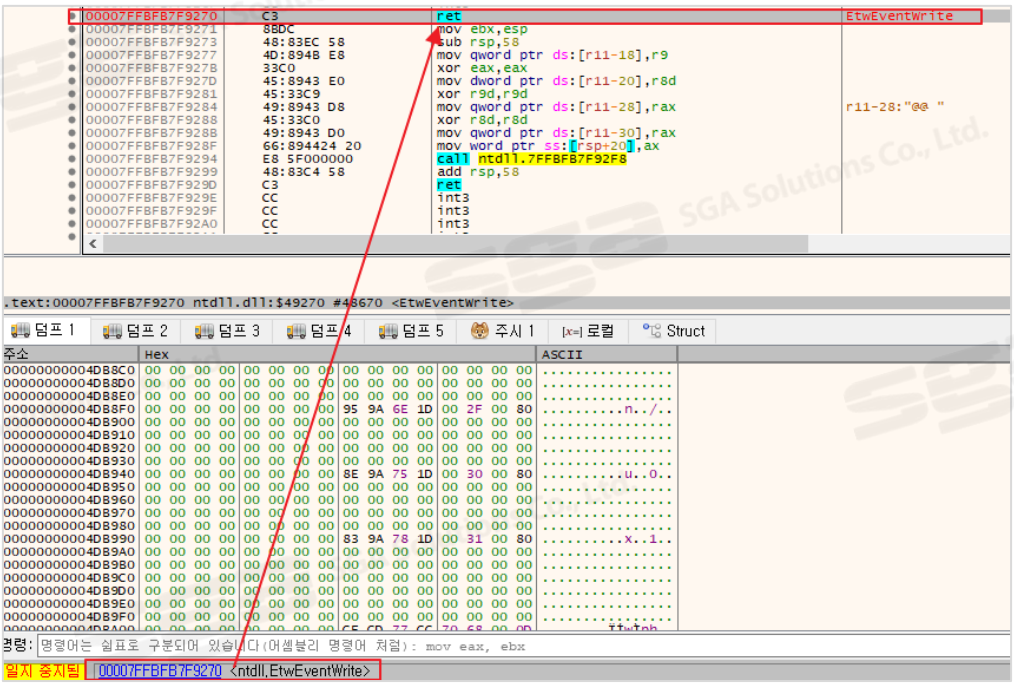
먼저 언어를 확인할 수 있는 API GetUserDefaultUILanguage의 반환 값이 러시아의 언어(0x419)인 경우에 실행을 즉시 중단한다. 이어서 지역을 확인할 수 있는 API GetUserGeoID의 반환 값이 필리핀(0xC9)인 경우에도 중단한다.

암호화 제외 조건인 언어와 지역 두 가지의 연관성에 대해 현재 알려진 정보는 없으나, GetUserGeoID의 반환 값 중 러시아 지역은 0xCB으로 확인된다.

중복 실행 방지를 위해 CreateMutexW를 사용하여 "05b50cbc-5b50-bc05-50cb-05b50cbc05b5"로 뮤텍스를 생성한다.

옵션 값 “-nomutex" 파라미타를 사용하면 뮤텍스 생성을 생략하여 다중 실행을 진행할 수 있다.

- 암호화 전 사전 준비 - 1



[도우이벤트 추적(ETW) 비활성화]

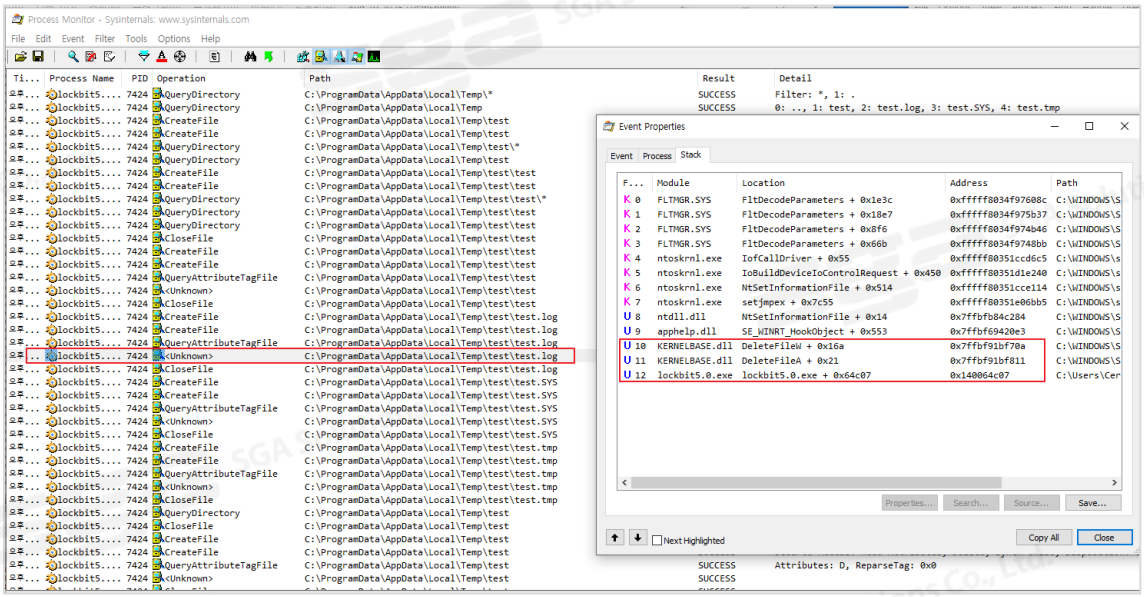
윈도우 이벤트 추적(ETW: Event Tracing for Windows) 기능에서 이벤트 데이터를 추적 세션에 기록하는 API EtwEventWrite 함수가 대상이다.

메모리 패치 방법은 EtwEventWrite 함수 주소의 첫 번째 바이트를 덮어씌우는 방식이며, 먼저 메모리 권한을 부여할 수 있는 NtProtectVirtualMemory API를 사용하여 메모리 영역 쓰기 권한을 변경한다.

이후 메모리에서 패치를 진행할 수 있는 NtWriteVirtualMemory API을 사용하여, 반환 명령어 RET(0xC3)을 이용하여 해당 주소에 첫 번째 바이트를 덮어쓴다. 결과적으로 해당 함수 EtwEventWrite를 호출하면 즉시 반환되며, ETW 기반 이벤트 수집이 사실상 비활성화된다.

이전 Lockbit 4.0에서는 RET 0x14(0xC2 0x14 0x00)이 사용되었으나 이번 LockBit 5.0에서는 더 간단한 RET(0xC3)으로 변경되었다.

- 암호화 전 사전 준비 - 2



[검색된 Temp 폴더 내부 파일 삭제]

원활한 암호화를 위해 Temp 폴더 내부를 탐색한 후 삭제하는 기능이 실행되며, 드라이브에서 시스템 내의 AppData\Local\Temp 폴더가 해당된다.

일반적으로 관리되지 않는 PC의 Temp 폴더엔 임시 파일이 다수 존재하며, 해당 내부 경로 내의 파일과 폴더를 삭제함으로써 암호화 효율을 높이는 것으로 판단된다.

또한 VSS(Volume Shadow Copy)는 볼륨의 스냅샷 백업 기능이며 많은 랜섬웨어들이 복구를 무력화하기 위해 삭제를 시도한다.

LockBit 5.0에서는 vssadmin, wmic 등의 커맨드 라인 도구를 사용하지 않고, COM을 초기화한 후에 CreateVssBackupComponentsInternal 등 VSS API를 직접 호출하는 방식으로 VSS 삭제를 진행한다.

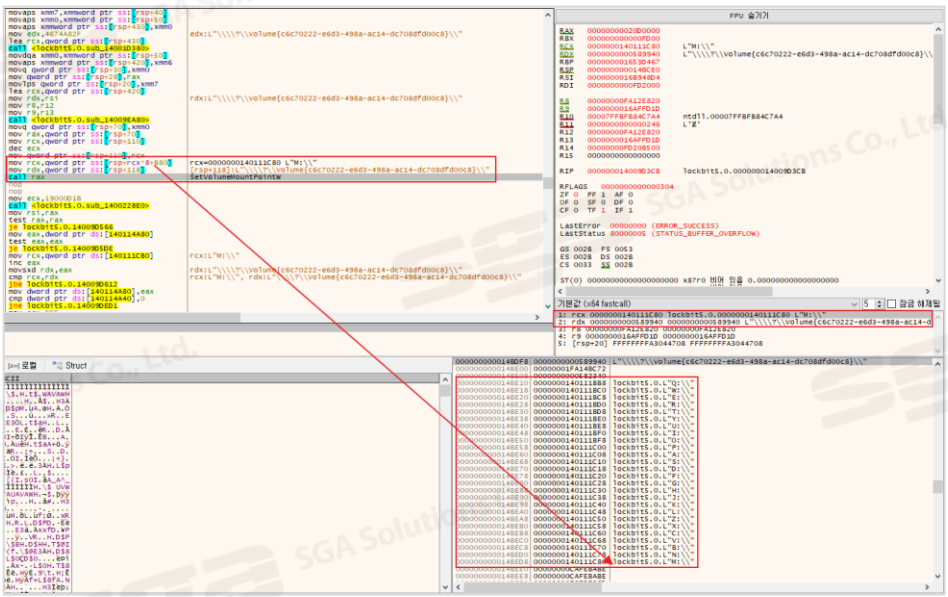
이후 서비스 종료 기능도 존재하며, 대상 서비스명은 평문이 아닌 해시값으로 하드코딩되어 저장된 값과 비교하기 때문에 정적 분석만으로 어떤 서비스가 대상인지 파악하기 어렵다는 특징이 있다.

따라서 삭제하는 대상 경로와 확인된 서비스는 다음과 같다.

대상 경로 패턴	설명
C:\ProgramData\AppData\Local\Temp*	TEMP 폴더 내부 파일/폴더 삭제 대상
C:\Users\<USERNAME>\AppData\Local\Temp*	
C:\Users\Default\AppData\Local\Temp*	
C:\Users\Default\AppData\Local\Temp*	
C:\Users\Public\AppData\Local\Temp*	

대분류	서비스/프로세스 목록
백업/복구	AcrSch2Svc, AcronisAgent, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, PDVFSService, backup, CAARCUpdateSvc, CASAD2DWebSvc, GxCIMgr, GxVss, gxcvd, gxfwd, gxblr, VeeamDeploymentService, VeeamNFSSvc, VeeamTransportSvc, stc_raw_agent, YooBackup, yooit, VSS, VSNAPVSS
보안/백신	RTVScan, SavRoam, defwatch, ccevtmgr, ccsetmgr, sophos, zhudongfangyu
DB/ERP	Intuit.QuickBooks.FCS, QBCFMonitorService, QBFCService, QBIDPService, sql
Microsoft/시스템	MicrosoftEdgeElevationService, edgeupdate, edgeupdatem, WSearch, vmms, svc$
메일서버	memtas, mepocs
unknown	0xdcf04e8c

- 드라이브 확인 및 마운트



[드라이브 마운트 매칭]

LockBit 5.0은 마운트 되지 않은 드라이브까지 암호화 대상에 포함시키기 위해 시스템의 모든 볼륨을 열거한 뒤 SetVolumeMountPointW API를 사용하여 해당 드라이브를 마운트 한다.

이는 시스템 전체에 대한 암호화 범위를 극대화하기 위한 기능으로 확인되며, 암호화 제외 목록에서 걸러진 암호화 대상 파일들은 암호화가 진행된다.

암호화 알고리즘은 파일 데이터 암호화에 ChaCha20-Poly1305(대칭 암호화), 키 교환에 X25519, 키 도출 과정에 BLAKE2b 해시 함수의 조합으로 모든 플랫폼(Windows, Linux, ESXi)에서 동일하게 진행된다.

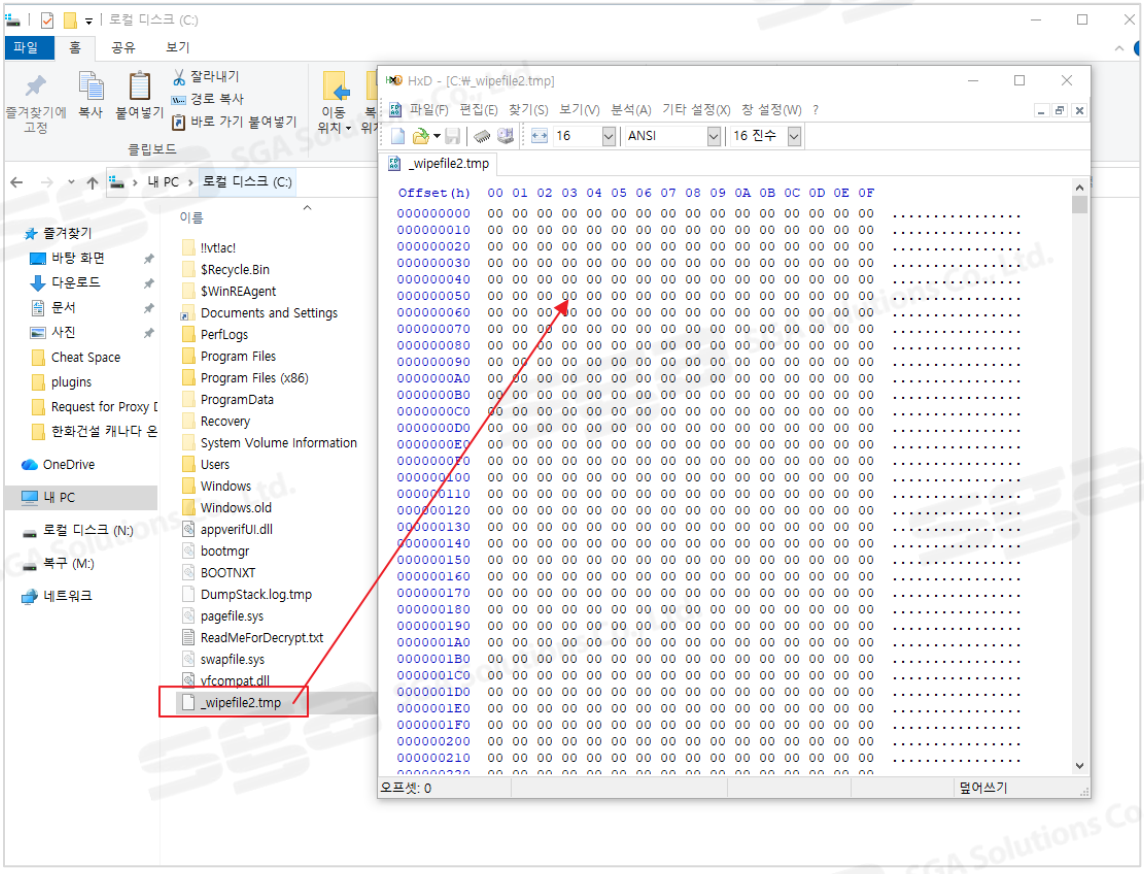
CPU 코어 수를 기반으로 암호화 스레드가 생성되며, 암호화가 완료된 파일에는 무작위로 생성된 16자리의 확장자가 추가된다.

전체 파일 암호화가 완료된 후에는 EvtClearLog API를 사용하여 윈도우 이벤트 로그 전체를 대상으로 삭제를 진행한다.

암호화 대상에서 제외되는 목록은 다음과 같다.

폴더명	파일명	파일 확장자
$Recycle.Bin, AllUsers, Boot, chocolatey, Microsoft Office, Microsoft Visual Studio, Windows Kits, WindowsApps, VisualStudio, System Volume Information, Microsoft\Windows, Windows\Hyper-V	iconcache.db, thumbs.db	.exe, .lnk, .dll, .cpl, .sy

- 와이퍼 기능 확인



[널 값을 이용한 포렌식 무력화]

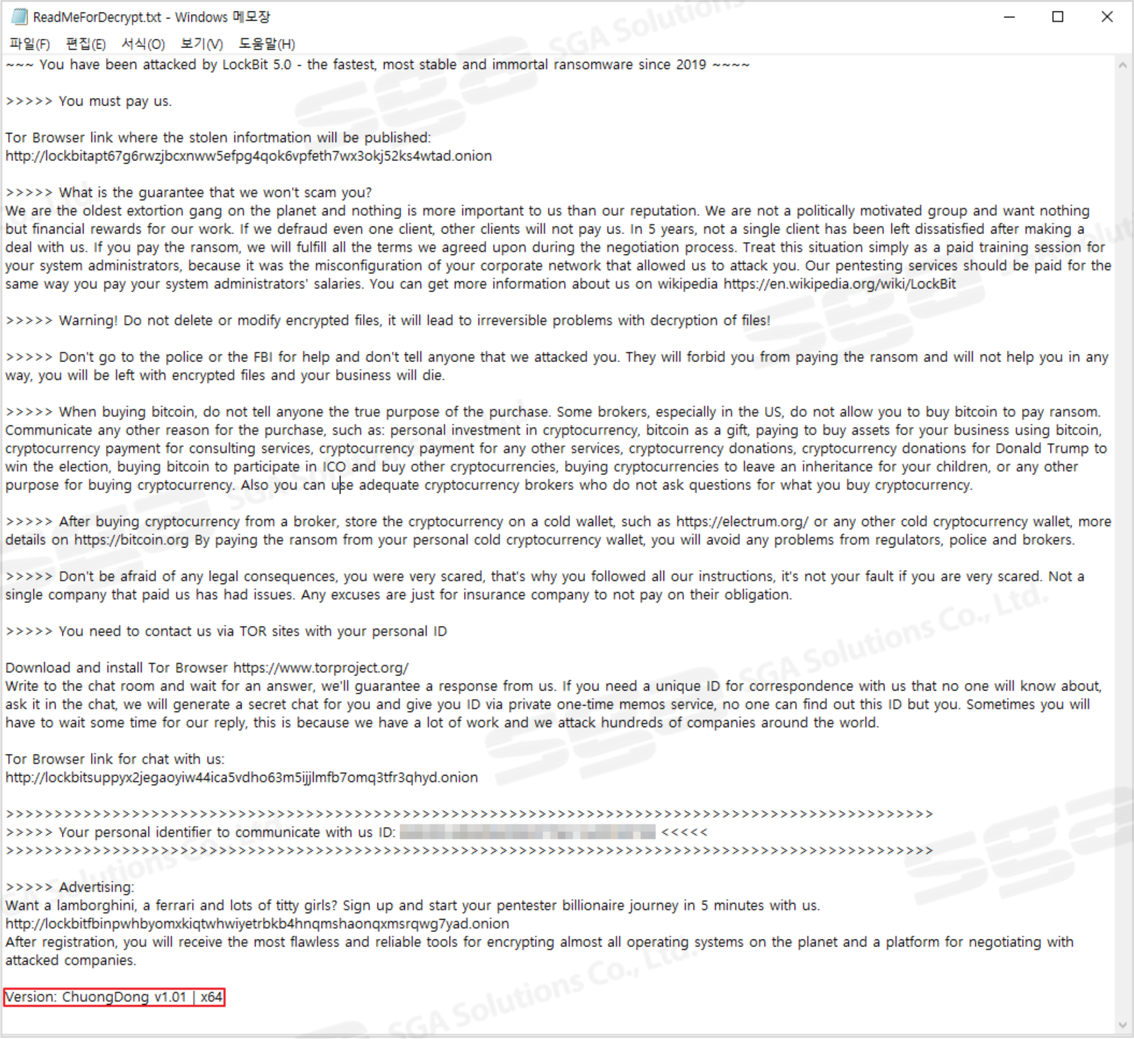
LockBit 5.0은 마운트 되지 않은 드라이브까지 암호화 대상에 포함시키기 위해 시스템의 모든 볼륨을 열거한 뒤 SetVolumeMountPointW API를 사용하여 해당 드라이브를 마운트 한다.

랜섬웨어 기능과 와이퍼 기능은 별도의 페이로드이며, 프로세스 할로잉 기법을 통해 자식 프로세스로 Defrag.exe를 생성 후 데이터 주입 및 실행한다.

루트 디스크(C:\)가 대상으로 파일 _wipefile1.tmp이 여유 공간 전체가 꽉 찰 때까지 널 데이터(0x00)로 가득 찬 4MB씩 반복 쓰기 실행하며 에러가 발생할 때까지 생성되고 삭제된다.

이후 동일한 방식으로 파일 _wipefile2.tmp이 생성되고 삭제되며 이와 같은 기능은 디스크 여유 공간의 포렌식 복구 차단 기능으로 확인된다.

- 랜섬 노트



```
ReadMeForDecrypt.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
~~~ You have been attacked by LockBit 5.0 - the fastest, most stable and immortal ransomware since 2019 ~~~~

>>>>> You must pay us.

Tor Browser link where the stolen infortmation will be published:
http://lockbitapt67g6rwzjbcxnww5efpg4qok6vpfeth7wx3okj52ks4wtad.onion

>>>>> What is the guarantee that we won't scam you?
We are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are not a politically motivated group and want nothing
but financial rewards for our work. If we defraud even one client, other clients will not pay us. In 5 years, not a single client has been left dissatisfied after making a
deal with us. If you pay the ransom, we will fulfill all the terms we agreed upon during the negotiation process. Treat this situation simply as a paid training session for
your system administrators, because it was the misconfiguration of your corporate network that allowed us to attack you. Our pentesting services should be paid for the
same way you pay your system administrators' salaries. You can get more information about us on wikipedia https://en.wikipedia.org/wiki/LockBit

>>>>> Warning! Do not delete or modify encrypted files, it will lead to irreversible problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you. They will forbid you from paying the ransom and will not help you in any
way, you will be left with encrypted files and your business will die.

>>>>> When buying bitcoin, do not tell anyone the true purpose of the purchase. Some brokers, especially in the US, do not allow you to buy bitcoin to pay ransom.
Communicate any other reason for the purchase, such as: personal investment in cryptocurrency, bitcoin as a gift, paying to buy assets for your business using bitcoin,
cryptocurrency payment for consulting services, cryptocurrency payment for any other services, cryptocurrency donations, cryptocurrency donations for Donald Trump to
win the election, buying bitcoin to participate in ICO and buy other cryptocurrencies, buying cryptocurrencies to leave an inheritance for your children, or any other
purpose for buying cryptocurrency. Also you can use adequate cryptocurrency brokers who do not ask questions for what you buy cryptocurrency.

>>>>> After buying cryptocurrency from a broker, store the cryptocurrency on a cold wallet, such as https://electrum.org/ or any other cold cryptocurrency wallet, more
details on https://bitcoin.org By paying the ransom from your personal cold cryptocurrency wallet, you will avoid any problems from regulators, police and brokers.

>>>>> Don't be afraid of any legal consequences, you were very scared, that's why you followed all our instructions, it's not your fault if you are very scared. Not a
single company that paid us has had issues. Any excuses are just for insurance company to not pay on their obligation.

>>>>> You need to contact us via TOR sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from us. If you need a unique ID for correspondence with us that no one will know about,
ask it in the chat, we will generate a secret chat for you and give you ID via private one-time memos service, no one can find out this ID but you. Sometimes you will
have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

Tor Browser link for chat with us:
http://lockbitsuppyx2jegaoyiw44ica5vdho63m5ijjlmfb7omq3tfr3qhyd.onion

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
>>>>> Your personal identifier to communicate with us ID: [redacted] <<<<<
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

>>>>> Advertising:
Want a lamborghini, a ferrari and lots of titty girls? Sign up and start your pentester billionaire journey in 5 minutes with us.
http://lockbitfbinpwhbyomxkiqtwhwiyetrbkb4hnqmshaonqxmsrqwg7yad.onion
After registration, you will receive the most flawless and reliable tools for encrypting almost all operating systems on the planet and a platform for negotiating with
attacked companies.

Version: ChuongDong v1.01 | x64
```

[랜섬 노트]

랜섬 노트에는 "Version: ChuongDong v1.01 x64"가 명시되어 있어 LockBit 5.0 버전은 ChuongDong 버전이라고도 불린다.

ChuongDong은 Mandiant FLARE 팀에서 재직 이력을 가진 리버스 엔지니어로 주요 랜섬웨어와 LockBit 4.0 블랙 버전을 상세 분석한 이력이 존재한다. LockBit 4.0 버전과 같은 해에 5.0으로 출시되었으며, 해당 분석가의 이름을 명시한 것은 분석 이력을 인지하고 의도적으로 기재한 것으로 판단된다.

5. 주요 보안 뉴스

'검색 수익화 솔루션 가장... 백신 제거해 2만5000개 시스템 위협 노출

'검색 수익화 기업'을 표방하는 드래곤보스솔루션(Dragon Boss Solutions LLC)이란 회사 소프트웨어가 정상적 업데이트 경로를 악용해 운영체제 최상위 권한(SYSTEM)을 장악뒤, 백신 제거 스크립트를 배포하는 공격을 가했다.

- 출처: https://www.boannews.com/media/view.asp?idx=143232&page=12&kind=4

"보안 도구가 도리어 흉기로"… 팀PCP, KICS 공급망 타격

해킹 그룹 팀PCP(TeamPCP)가 공식 도커 허브 저장소인 'checkmarx/kics'에 악성코드를 삽입한 가짜 이미지를 주입해 공급망 공격을 감행했다.

제이프로그(JFrog)와 소켓(Socket)이 23일 발표한 분석 보고서에 따르면, 오염된 바이너리는 인프라 코드(IaC: Infrastructure as Code) 스캔 보고서를 암호화해 외부로 빼돌리는 불법적인 정보 탈취 기능을 실행한다. 보안 도구로 널리 쓰이는 시스템이 해킹 도구로 돌변한 셈이다.

- 출처: https://www.boannews.com/media/view.asp?idx=143332&page=8&kind=1

SGA 보안레이더

에스지에이솔루션즈(주)

https://www.sgasol.kr

경기도 의왕시 광진말로 54, 의왕 스마트시티퀀텀 B동 5층 525호