Qilin Ransomware 분석

Genians ⋮ ⋮ 10/28/2025

◈ 주요 결과 (Key Findings)

- 2022년 후반부터 활동을 본격화한 후, 2024~2025년 들어 RaaS 운영 모델을 통해 위협 증가
- Golang 및 Rust 기반의 크로스 플랫폼 랜섬웨어가 사용되는 것으로 보고
- 단순 암호화에 그치지 않고 데이터 탈취 및 유포 협박(더블 익스토션)을 병행
- 행위 기반 탐지와 위협 인텔리전스 연계가 가능한 EDR 체계 강화가 핵심 대응 전략

1. 개요 (Overview)

Qilin은 별칭으로는 'Agenda' 랜섬웨어로도 알려져 있으며, 약 2022년 7월경 첫 출현이 보고된 이후 랜섬웨어 서비스 모델을 통해 다양한 조직을 공격해오고 있습니다.

이 조직은 기본적으로 '랜섬웨어 개발자 + 제휴 공격자(affiliates)' 형태의 RaaS 플랫폼을 운영하며, 제휴 공격자는 Qilin이 제공하는 인프라·툴을 이용해 공격을 수행하고 그 수익을 나누는 구조를 갖고 있습니다.

최근에는 제휴 모집 기능 강화, 자동화 기능 추가, 다양한 플랫폼 지원 등으로 공격 역량을 확장하였고, 이로 인해 전세계 다양한 산업군에 피해를 주고 있는 상태입니다.

2. 배경 (Background)

2-1. 랜섬웨어 조직 및 운영 형태

Qilin은 러시아어권 언더그라운드 포럼에서 제휴 모집 공고가 확인된 바 있으며, 러시아 또는 독립국가연합(CIS) 지역 기반일 가능성이 거론됩니다. 제휴수익 구조는 보고에 따라 다른데, 일부 자료에서는 중-소 규모 금액에 대해 제휴자가 약 80 %를 가져가고 운영측이 15~20 %를 가져가는 구조로 설명됩니다.

랜섬웨어 생태계 측면에서 보면, 기존 강세였던 다른 RaaS 조직(RansomHub, LockBit 등)이 내부 붕괴나 운영상 문제를 겪는 사이 Qilin이 그 공백을 빠르게 메우며 활동량을 증가시킨 것으로 분석됩니다.

더불어 Qilin은 러시아어권 기반 + 홍콩 등지에 법인을 둔 방탄호스팅(Bulletproof Hosting, 이하 BPH) 제공업체 네트워크와 긴밀히 연결되어 있다는 보고가 있습니다. Qilin은 피해 조직의 데이터를 유출 위협하며, 이 DLS(Data Leak Site)가 주로 BPH 인프라 상에 호스팅되어 있습니다.

2-2. 활동 동향

2023년에는 주로 수백만 달러 이하(예: 5만 ~ 80 만 달러) 규모의 요구가 많았던 반면, 2024년 이후로 공격 규모 및 요구액이 증가 추세입니다. 2024년 6월에는 영국의 병원 관련 의료검사기관인 Synnovis을 통해 큰 의료서비스 중단을 일으키는 등 현실 세계에까지 영향을 미친 공격이 보고되었습니다.

2025년 4월에는 글로벌 랜섬웨어 공격 수가 감소하는 흐름에서도 Qilin은 공격 건수 측면에서 가장 활발한 그룹 중 하나로 부상했습니다. 특히 최근 일본의 아사히 그룹 공격 사례가 확인되었습니다.

2-3. 기술적 특징

Qilin은 Golang으로 개발된 초기 버전에 이어 Rust 기반 버전도 확인된 바 있으며, 이는 실행 효율성·은폐성 향상을 위한 것으로 보입니다. Windows 및 Linux 양쪽 플랫폼을 노리며, 특히 VMware vCenter·ESXi 같은 가상화 인프라에 대한 타깃화가 두드러집니다.

암호화 알고리즘으로는 ChaCha20, AES-256, RSA-4096 등이 보고되어 있으며, 다양한 모드로 실행옵션이 구성되어 있습니다. 실행 조건에 '비밀번호(password) 인자 요구' 방식이 포함되며, 샌드박스 회피 또는 분석 회피 기법으로 사용됩니다. 암호화 시 쉐도우 카피본 삭제, 이벤트 로그 클리어, 프로세스 종료, 도메인 내 확산, 디스크 이미지 마운트/언마운트 등의 후속 행동이 확인됩니다.

2-4. 공격 수법 및 침입 경로

초기 접근에는 스피어 피싱(메일 첨부·링크), 노출된 원격접속(RDP, 원격관리 솔루션) 또는 백업/클라우드 관련 소프트웨어의 취약점 이용 등이 확인됩니다. 예컨대, Veeam Backup & Replication의 CVE-2023-27532 취약점을 이용한 접근이 보고된 바 있습니다.

제휴 패널을 통한 공격자 환경 설정이 가능한데, 예컨대 제외할 디렉토리/파일 목록, 서비스 종료 목록, 회사ID 기반의 확장자 설정 등 피해자 맞춤형 구성이 가능하게끔 설계되어 있습니다.

2-5. 피해 및 영향

단발적인 암호화 피해에 그치지 않고 데이터 탈취와 유포 위협(또는 실제 유출) 형태의 '더블 익스토션(Double Extortion)' 전략이 핵심입니다. 피해 규모는 수십 만 달러에서 수백만 달러까지 요구된 사례가 있으며, 2024년 이후에는 고액화·고위험화 흐름이 강화된 것으로 보입니다. 특히 중요 인프라(예: 의료기관)에서의 공격은 실제 운영 중단, 인명 피해 가능성까지 제기될 정도로 위협적입니다.

3. 일본 공격 사례 분석

3-1. 다크웹 포털 기반 공개 협박

2025년 9월 29일경 일본 아사히 그룹이 디지털 주문·출하·고객서비스 시스템 장애를 겪었으며, 이후 Qilin이 해당 공격을 자처하고 약 9,300여 건의 파일(약 27GB) 탈취를 주장했습니다.

Log In

← Back

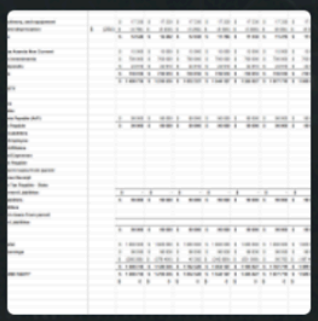
ASAHI GROUP HOLDINGS, LTD.

Asahi Group Holdings, Japan - a leading manufacturer of beer and non-alcoholic beverages in Japan. Asahi is headquartered in Sumida, Tokyo. It ranked 593rd on the Forbes Global 2000 list of the world's largest companies in 2023. The company's annual revenue is approximately $18.6 billion. Asahi Group Holdings established in 1889 that offers a global portfolio of alcoholic and non-alcoholic beverages, food, and other products, including brands like Asahi Super Dry, Peroni, Pilsner Urquell, and Grolsch. There was a global disruption in the company's operations. Immediately 6 breweries of the company stopped their work, a total of 30 enterprises of the company were affected. Analysts have estimated that if the company is unable to fix all working processes by the end of the month, Asahi will have to reduce its operating profit forecast for the fourth quarter by 83% in Japan and 38% worldwide. The company will lose from $200 million to $335 million. The reason is a global information leak. The leak affected financial documents, budgets and contracts, as well as personal data of employees, plans and development forecasts of the company. Part of this information is already available in the public domain.

COMPANY URL | OCT 7, 2025 | 10548

29 photos | 9323 files | 27.00 GB

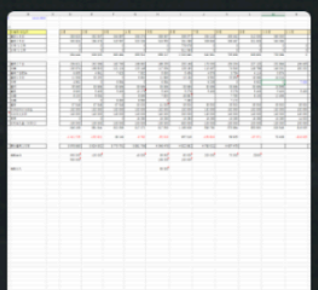
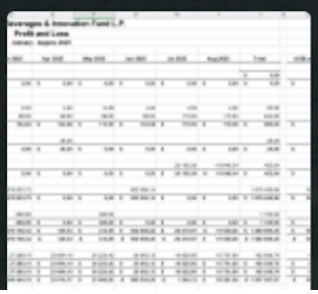
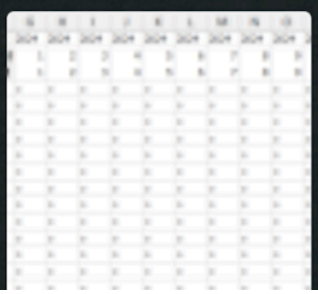
// IMAGES





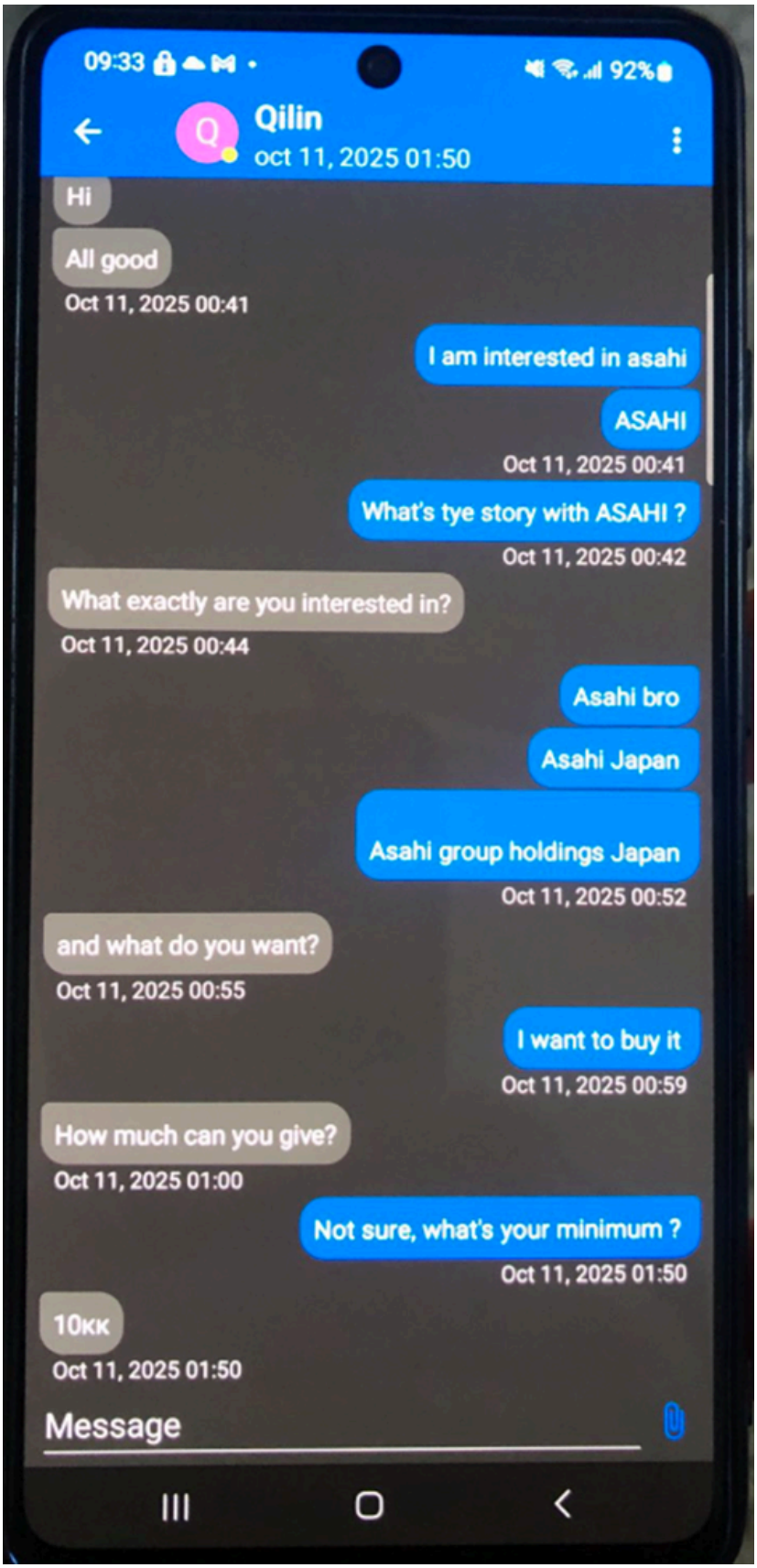


[사진 3-1] Qilin 다크웹 협박 화면

아사히 그룹은 일본 내 제조·출하망이 마비됨으로써 일부 생산라인 및 물류에 지장을 겪었고, 국내 소비자용 음료·주류 공급이 일시적으로 차질을 빚었다는 보도가 나왔습니다. Qilin은 공격 직후 자사 데이터 유출사이트에 아사히 그룹 관련 문서 스크린샷 및 내부자료 일부 게시했으며, 이로 인해 '제조·물류 대상 고급타겟'으로의 공격 역량이 실증된 셈입니다.

Resecurity에 따르면, Qilin 운영자들과 비공개 대화를 나누었고 위협 행위자들이 도난당한 Asahi 데이터를 1,000만 달러에 판매하려 한다는 사실을 공개했습니다.



[사진 3-2] 대화 메시지 화면 (출처 : Resecurity)

3-2. 랜섬웨어 동작 과정

변종에 따라 다를 수 있지만, Qilin 랜섬웨어는 실행 인자로 전달된 '--password' 값의 유효성 검사 및 통과 후에만 페이로드를 활성화하도록 설계되어 있습니다.

입력된 문자열은 SHA256 해시 알고리즘으로 바이너리 내부에 하드코딩된 SHA256 계열 해시값과 비교합니다. 비교가 성공하면 암호화 루틴이 트리거 됩니다. 일반적으로 비밀번호 기반 랜섬웨어는 입력값을 암호화/복호화 키로 사용하여 자체 코드 또는 구성 데이터를 복호화한 뒤 실제 악성 행위를 수행하는 반면, Qilin의 구현은 이미 실행 가능한 형태로 존재하는 구조를 취하고 있습니다.

랜섬웨어는 사고 대응과 시스템 복구를 방해하기 위해 이벤트 로그 및 백업 관련 데이터를 의도적으로 제거하는 행위를 수행합니다. 분석대상 샘플은 Windows의 볼륨 섀도 복사본을 제거하기 위해 vssadmin.exe를 활용하며, 삭제를 완결시키기 위해 일련의 서비스 조작 절차를 실행합니다.

구체적으로는 VSS 서비스(Volume Shadow Copy Service)의 시작 유형을 변경하여 수동으로 전환한 뒤 서비스를 실행하고, 그 상태에서 섀도 복사본 삭제 명령을 호출하여 존재하는 백업 스냅샷을 제거합니다. 삭제 완료 후에는 VSS 서비스를 중지시키고 시작 유형을 사용 안 함(또는 무효화) 상태로 되돌려 추후 자동 복구 가능성을 차단합니다.

이러한 절차는 포렌식 흔적을 감소시키고 복구 수단을 제한함으로써 사고 분석과 데이터 복구를 어렵게 만드는 목적을 가집니다.

- **서비스 시작 유형을 수동(Manual) 으로 변경**
-
    - wmic service where name='vss' call ChangeStartMode Manual
        - *VSS 서비스가 자동으로 실행되지 않도록 시작 정책을 수동으로 변경합니다.*
- **VSS 서비스 시작**
-
    - net start vss
        - *섀도 복사본 삭제 명령을 실행하기 위해 VSS 서비스를 일시적으로 기동합니다.*
- **모든 섀도 복사본을 조용히 삭제**
-
    - vssadmin.exe delete shadows /all /quiet
        - *존재하는 모든 볼륨 섀도 복사본(백업 스냅샷)을 사용자 확인 없이 삭제합니다.*
- **VSS 서비스 중지**
-
    - net stop vss
        - *삭제 작업 종료 후 서비스를 중지하여 즉시 동작을 멈춥니다.*
- **서비스 시작 유형을 사용 안 함(Disabled) 으로 변경**

-
    - wmic service where name='vss' call ChangeStartMode Disabled
        - *향후 자동 재시작을 방지하기 위해 서비스 시작 정책을 비활성화합니다.*

이후 실행되는 PowerShell 스크립트는 시스템의 모든 이벤트 로그 채널을 열거하여 백업 절차 없이 각 채널의 이벤트 레코드를 즉시 초기화합니다. 이 작업은 PowerShell에서 제공하는 기능과 함께 .NET 클래스인 System.Diagnostics.Eventing.Reader.EventLogSession을 호출하여 수행되며, 관리자 권한으로 실행해야 하고 Security 로그 등 일부 채널은 추가적인 시스템 권한이나 권한 상승이 필요할 수 있습니다.

로그 초기화로 기존 로그는 표면상 제거되지만 삭제 행위 자체의 기록, 디스크 잔여 데이터, 백업 이미지, 또는 중앙집중형 로그 수집본에는 흔적이 남을 가능성이 있어 완전 복구가 불가능하다고 단정할 수 없습니다. 이러한 로그 초기화 행위는 포렌식 추적을 저해하고 사고 대응을 지연시키는 전형적인 안티포렌식 기법입니다.

더불어 레지스트리 등록을 통해 자체 지속성을 확보합니다. 이때 레지스트리의 값 이름은 랜덤하게 생성된 6문자 문자열 앞에 * 문자가 붙는 형식으로 구성되며, 내부 실행 로직은 값 이름에 * 접두사가 있을 경우 안전 모드(Safe Mode)에서도 페이로드를 실행하도록 설계되어 있습니다.

한편, 실행 인자로 '--no-destruct'를 명시하지 않으면 랜섬웨어는 자체 삭제(self-destruct) 동작을 수행하므로 실행 완료 후에는 실행 파일이 제거되고 레지스트리의 값만 남게 됩니다. 이 경우 실행 파일이 제거된 상태에서는 재부팅 이후 레지스트리 항목만으로는 페이로드가 재실행되지 않으므로 지속성이 사실상 상실됩니다.

파일 암호화 성공률을 극대화하고 복구 절차를 방해하기 위해 암호화 수행 이전에 목표 서비스들을 선제적으로 중단하고 해당 서비스의 시작 유형을 사용 안 함(Disabled)으로 변경합니다. 대상 서비스는 서비스 이름 또는 설명 문자열을 기반으로 식별(부분 문자열 매칭)하며, 식별된 서비스에 대해 중지 명령을 발행한 후 자동 재시작을 방지하기 위해 시작 유형을 변경하는 방식으로 동작합니다. 공격 대상 목록에는 관계형 데이터베이스(MSSQL), 메일 서버(Exchange), 가상화 플랫폼(Hyper-V), 대표적 백업 제품군(Acronis, Commvault, Veeam, Veritas Backup Exec), 회계·ERP(QuickBooks, SAP), 그리고 일부 엔드포인트/서버 보안솔루션(Sophos) 등이 포함되어 있습니다. 이러한 행위는 파일이 잠기거나 백업이 동작하여 암호화가 차단되는 상황을 회피하려는 목적이며, 서비스 중지와 시작 유형 변경은 관리자 권한 이상이 필요합니다.

데이터 암호화 과정에서도 Qilin은 반복적으로 실행 중인 프로세스를 스캔하여 암호화 작업을 방해할 수 있는 프로세스를 강제 종료합니다. 이 동작은 서비스 중단과 동일한 의도로 수행되며, 대상은 데이터베이스, 백업·복구 에이전트, 가상화 관련 프로세스 및 보안 솔루션 프로세스 등 파일 접근을 유지하거나 복구를 수행할 수 있는 항목들입니다.

내부적으로는 프로세스 이름 또는 실행 경로의 문자열 매칭을 통해 대상을 식별하고 주기적으로 검사하여 일치하는 프로세스에 대해 종료를 반복하는 방식으로 보입니다. 이러한 프로세스 종료는 열린 파일 핸들로 인한 암호화 실패를 줄이고 복구 수단을 차단하기 위한 조치이며, 정상적으로는 관리자 권한 이상이 필요합니다.

```
[07:45:15|+0.00711204] <ThreadId(1)>: process_black_list: ["vmms", "vmwp", "vmcompute", "agntsvc", "dbeng50", "dbsnmp", "encsvc", "excel", "firefox", "infopath", "isqlplussvc", "sql", "msaccess", "mspub", "mydesktopqos", "mydesktopservice", "notepad", "ocautoupds", "ocomm", "ocssd", "onenote", "oracle", "outlook", "powerpnt", "sqbcoreservice", "steam", "synctime", "tbirdconfig", "thebat", "thunderbird", "visio", "winword", "wordpad", "xfssvccon", "bedbh", "vxmon", "benetns", "bengien", "pvlsvr", "beserver", "raw_agent_svc", "vsnapvss", "cagservice", "qbidpservice", "qbdbmgrn", "qbcfmonitorservice", "sap", "teamviewer_service", "teamviewer", "tv_w32", "tv_x64", "cvmountd", "cvd", "cvfwd", "cvods", "saphostexec", "saposcol", "sapstartsrv", "avagent", "avscc", "dellsystemdetect", "enterpriseclient", "veeamnfssvc", "veeamtransportsvc", "veeamdeploymentsvc", "mvdesktopservice"]
[07:45:15|+0.00737317] <ThreadId(1)>: win_services_black_list: ["vmms", "mepocs", "memtas", "veeam", "backup", "vss", "sql", "msexchange", "sophos", "msexchange", "msexchangeWW$", "wsbexchange", "pdvfsservice", "backupexecvssprovider", "backupexecagentaccelerator", "backupexecagentbrowser", "backupexecdivecimediaservice", "backupexecjobengine", "backupexecmanagementservice", "backupexecrpcservice", "gxblr", "gxvss", "gxclmgrs", "gxcvd", "gxcimgr", "gxmmm", "gxvsshwprov", "gxfwd", "sapservice", "sap", "sapWW$", "sapdWW$", "saphostcontrol", "saphostexec", "qbcfmonitorservice", "qbdbmgrn", "qbidpservice", "acronisagent", "veeamnfssvc", "veeamdeploymentservice", "veeamtransportsvc", "mvarmor", "mvarmor64", "vsnapvss", "acrsch2svc", "(.*?)sql(.*?)"]
```

[사진 3-3] 종료 대상 프로세스 및 서비스

시스템 손상을 방지하기 위해 암호화 대상에서 제외되는 특정 파일 확장자와 파일, 그리고 경로를 별도로 정의합니다. 이러한 예외 목록은 운영체제 핵심 파일이나 주요 애플리케이션 파일을 보호하여, 잘못된 암호화로 인해 시스템 기능이 저하되거나 부팅이 불가능해지는 상황을 예방하는 역할을 합니다.

```
[07:45:15|+0.00606629] <ThreadId(1)>: extension_black_list: ["themepack", "nls", "diapkg", "msi", "lnk", "exe", "scr", "bat", "drv", "rtp", "msp", "prf", "msc", "ico", "key", "ocx", "diagcab", "diagcfg", "pdb", "wpx", "hlp", "icns", "rom", "dll", "msstyles", "mod", "ps1", "ics", "hta", "bin", "cmd", "ani", "386", "lock", "cur", "idx", "sys", "com", "deskthemepack", "shs", "theme", "mpa", "nomedia", "spl", "cpl", "adv", "icl", "msu", "5I_Y_Pz8PK"]
[07:45:15|+0.00623825] <ThreadId(1)>: extension_white_list: ["mdf", "ldf", "bak", "vib", "vbk", "vbm", "vrb", "vmdk", "abk", "bkz", "sqb", "trn", "backup", "bkup", "old", "tibx", "pfi", "pvhd", "pbf", "dim", "gho", "vpcbackup", "arc", "mtf", "bkf", "dr"]
[07:45:15|+0.00641162] <ThreadId(1)>: filename_black_list: ["desktop.ini", "autorun.ini", "ntldr", "bootsect.bak", "thumbs.db", "boot.ini", "ntuser.dat", "iconcache.db", "bootfont.bin", "ntuser.ini", "ntuser.dat.log", "autorun.inf", "bootmgr", "bootmgr.efi", "bootmgfw.efi", "#recycle", "autorun.inf", "boot.ini", "bootfont.bin", "bootmgr", "bootmgr.efi", "bootmgfw.efi", "desktop.ini", "iconcache.db", "ntldr", "ntuser.dat", "ntuser.dat.log", "ntuser.ini", "thumbs.db", "#recycle", "bootsect.bak"]
[07:45:15|+0.00655979] <ThreadId(1)>: directory_black_list: ["windows", "system volume information", "intel", "admin$", "ipc$", "sysvol", "netlogon", "$windows.~ws", "application data", "mozilla", "program files (x86)", "program files", "$windows.~bt", "msocache", "tor browser", "programdata", "boot", "config.msi", "google", "perflogs", "appdata", "windows.old", "appdata", "..", ".", "boot", "windows", "windows.old", "$recycle.bin", "admin$"]
[07:45:15|+0.00682058] <ThreadId(1)>: white_symlink_dirs: []
[07:45:15|+0.00696496] <ThreadId(1)>: white_symlink_subdirs: ["ClusterStorage"]
```

[사진 3-4] 암호화 제외 대상 파일, 확장자 및 경로

파일 암호화 과정은 먼저 암호화에서 제외할 경로, 파일, 확장자를 확인하는 단계로 시작합니다. 이후 파일 암호화에 사용할 알고리즘을 선택하며, 사용되는 알고리즘은 AES-256과 ChaCha20 두 가지로 구분됩니다. 기본적으로 파일은 대칭키 방식인 AES-256으로 암호화되며, 이 대칭키는 RSA-4096 공개키로 다시 암호화됩니다.

단, 피해 시스템이 AES-NI(Advanced Encryption Standard-New Instructions)를 지원하지 않는 경우에는 AES-256 대신 ChaCha20 알고리즘이 사용됩니다. AES-NI 미지원 환경은 대체로 2011년 이전 출시된 구형 CPU이거나, 메인보드에서 AES-NI 기능이 제공되더라도 BIOS 설정에서 비활성화된 경우를 포함합니다.

모든 준비가 완료되면 파일 전체 데이터를 암호화하며, 암호화된 데이터 구간의 끝에는 "-----END CIPHERTEXT BLOCK-----" 문자열이 삽입되어 구간 경계를 명확히 표시합니다. 또한 암호화된 데이터의 시작 부분에는 최대 512바이트까지 원본 데이터 일부가 삽입됩니다.

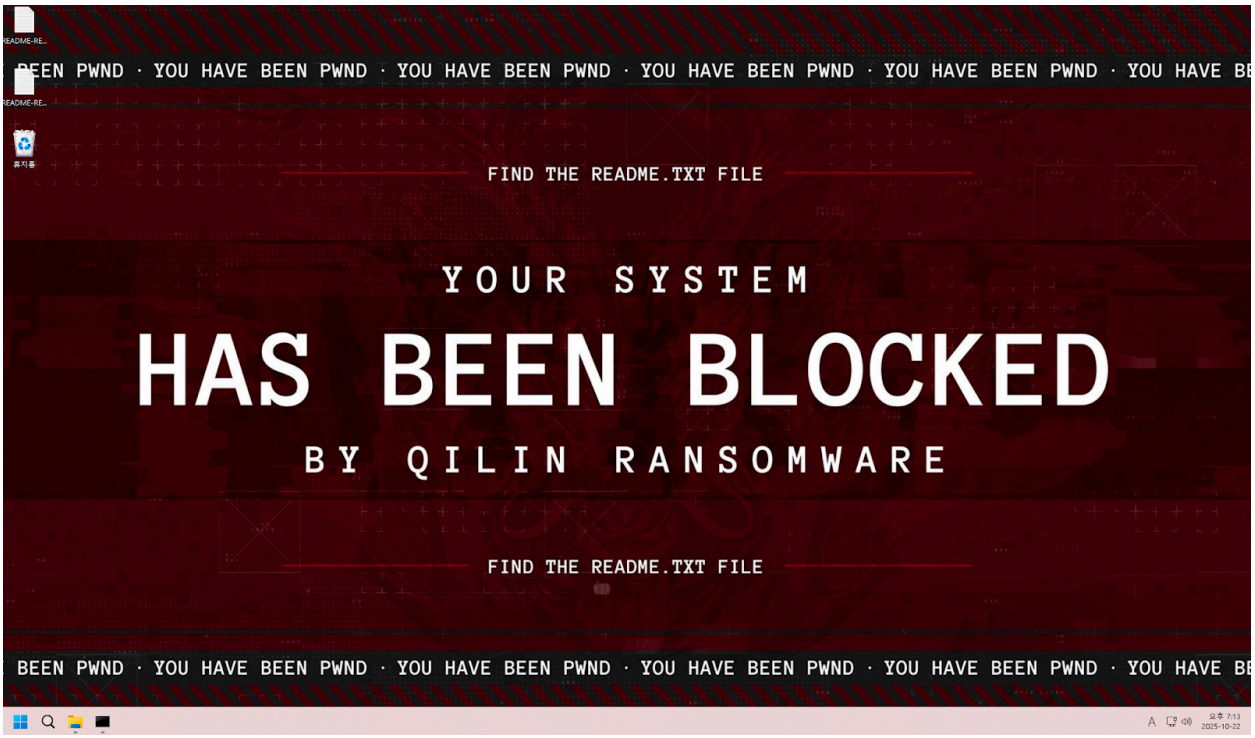
최종 파일 구조는 다음과 같이 구성됩니다. 암호화된 데이터 + 암호화된 키 데이터 + 끝을 알리는 문자열 + 암호화된 데이터 (최대 512바이트) 형태로 구성됩니다. 이 구조로 인해 로컬 환경에서는 파일을 복호화할 수 있는 유효한 단서가 남지 않으며, 피해자는 별도의 복호화 키 없이는 파일 접근이 불가능하게 됩니다.

[사진 3-5] 암호화 제외 대상 확장자 및 경로

3-3. 랜섬웨어 감염 현상

하기 화면은 Qilin 랜섬웨어에 의해 감염된 상태를 보여주며 바탕화면이 공격자가 지정한 이미지로 교체되어 있음을 확인할 수 있습니다. 랜섬웨어는 바탕화면 교체를 통해 피해자에게 즉각적인 시각적 인지를 유도하고, 복구 요구사항을 포함한 랜섬노트 내용을 안내하고, 공격자와의 소통을 강요하는 사회공학적 기능을 수행합니다.

또한 바탕화면 변경은 단순한 UI 조작을 넘어 레지스트리와 파일 시스템 상에 흔적을 남기므로 포렌식 분석 시 해당 키와 파일의 생성·수정 시간, 소유자 정보, 파일 해시 등을 수집하면 감염 시점과 공격 행위의 연계 증거 확보에 유용합니다.



[사진 3-6] 랜섬웨어로 변경된 바탕화면

랜섬노트는 README-RECOVER-<암호화 확장자>.txt 형식의 파일명으로 생성되며, 분석 대상 샘플에서는 식별자가 노트 내 식별자(victim ID) 및 접근 계정으로 사용됩니다. 랜섬노트는 암호화 제외 경로를 제외한 대부분의 디렉터리에 우선적으로 생성되므로 시스템 전역에 걸쳐 다수의 복사본이 남게 되고, 결과적으로 포렌식 수집 시 노트 파일의 생성·수정 시각과 소유자, 파일 해시를 이용해 감염 범위 및 초기 감염 시점을 파악하는 데 유용한 지표가 됩니다.

랜섬노트 본문에는 공격자가 시스템 및 네트워크에서 민감 데이터를 수집했으며, 피해자와의 협상이 결렬될 경우 해당 자료를 공격자가 운영하는 다크웹에 게시하겠다는 협박성 문구가 포함됩니다. 피해자는 랜섬노트에 기재된 식별자와 비밀번호를 이용해 DLS에 접속하라는 지시를 받으며, 이 과정은 단순한 파일 암호화 통지에서 더 나아가 데이터 유출을 전제로 한 이중갈취(double extortion) 위협을 수반합니다.

README-RECOVER-5I_Y_Pz8I

파일 편집 보기

-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from your system/network.
Our group cooperates with the mass media.
If you refuse to communicate with us and we do not come to an agreement, your data will be reviewed and published on our blog and on the media page (https://wikileaks2.site/)

Blog links:
http://[redacted]
http://[redacted]

Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decisions.

-- Recovery

1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials

Please note that communication with us is only possible via the website in the Tor browser, which is specified in this note.
All other means of communication are not real and may be created by third parties, if such were not provided in this note or on the website specified in this note.
-- Credentials

줄 31, 열 1 | 1,833자 | 100% | Windows (CRLF) | UTF-8

[사진 3-7] 랜섬노트 화면

4. 결론 및 대응 (Conclusion)

Qilin은 현재 랜섬웨어 생태계에서 가장 주목해야 할 위협 중 하나입니다. RaaS 운영 모델을 통해 제휴 공격자를 광범위하게 모집하고 있고, 기술적 완성도와 공격 규모·속도 측면에서도 급격히 성장하고 있습니다.

특히 고가치공격(high-value target)을 노리고 있으며, 단순 피해를 넘어 실질적인 운영 중단 및 데이터 유출 위협까지 병행하고 있다는 점이 특징입니다. 한국, 일본을 포함한 아시아·태평양 지역 조직도 잠재적 타깃이므로, 보안팀에서는 이 조직에 대해 대비 강화를 고려할 필요가 있습니다.

아래는 Qilin을 포함한 유사 랜섬웨어 조직에 대응하기 위한 권고사항으로, 분석업무 및 보안체계 수립에 참고가 될 수 있습니다.

4-1. 초기접근 차단 강화

- 스피어 피싱 메일 대비 교육 및 모의훈련을 정기적으로 실시할 것
- RDP/원격관리, 외부 접속 포트 등 노출된 서비스에 대한 접근제어(2차 인증, IP제한 등)를 강화할 것
- 백업·클라우드솔루션, 원격관리도구 등에서의 알려진 취약점(CVE) 모니터링 및 패치 체계 확보

4-2. 네트워크 및 엔드포인트 방어 강화

- EDR 솔루션 도입·구축을 통해 의심행위(프로세스 종료, 섀도우 볼륨카피 삭제, 이벤트로그 클리어 등) 감시 강화
- 내부망 분리(segmentation) 및 권한 최소화 정책을 통해 수평이동(lateral movement)을 어렵게 만들 것
- 백업 시스템 포함한 중요 자산의 오프라인 또는 격리된 상태에서의 백업 전략 수립 및 정기적인 복구 시험

4-3. 탐지 및 완화 조치

- 비정상 네트워크 활동 및 C2 통신 탐지 체계를 구축하고, 특히 제휴형 랜섬웨어 조직이 사용하는 토르(Tor) 기반 DLS 또는 C2 인프라 연계 가능성에 주의
- 사건 발생 시 '데이터 탈취' 가능성까지 고려한 대응계획(Ransomware + Exfiltration) 마련
- 위협 인텔리전스를 통해 Qilin 관련 최신 TTPs(기법·절차)를 지속 모니터링하고, 내부 보안팀과 공유

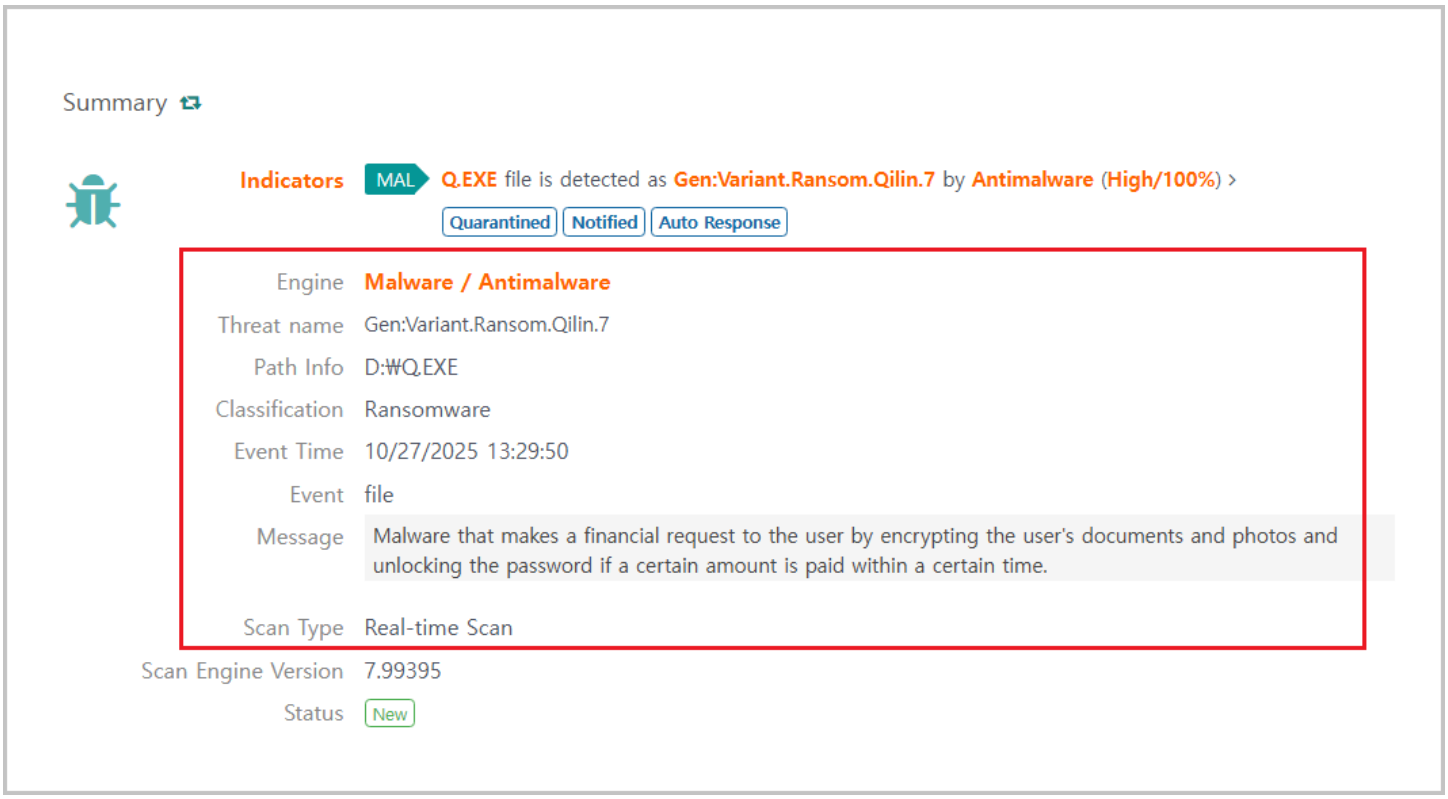
4-4. 사고 대응 및 복구 준비

- 랜섬노트 발견 시, 즉시 격리 및 외부 통신 차단, 로그 확보, 포렌식 대응 흐름 준비
- 피해 발생 시 납부 여부를 판단하기 전에 포렌식 증거 확보
- 법률/보험/법집행 기관 연계 업무 협력 절차를 사전 확보

- 복구절차에 있어서는 암호화된 데이터 복원 가능 여부, 백업 무결성 확인, 복구 우선순위 설정 등이 포함

Genian EDR은 Anti-Malware 및 Anti-Ransomware 엔진을 통해 랜섬웨어 시그니처 기반 탐지뿐만 아니라 시그니처 유사도 분석을 통한 변종 랜섬웨어 탐지가 가능합니다.

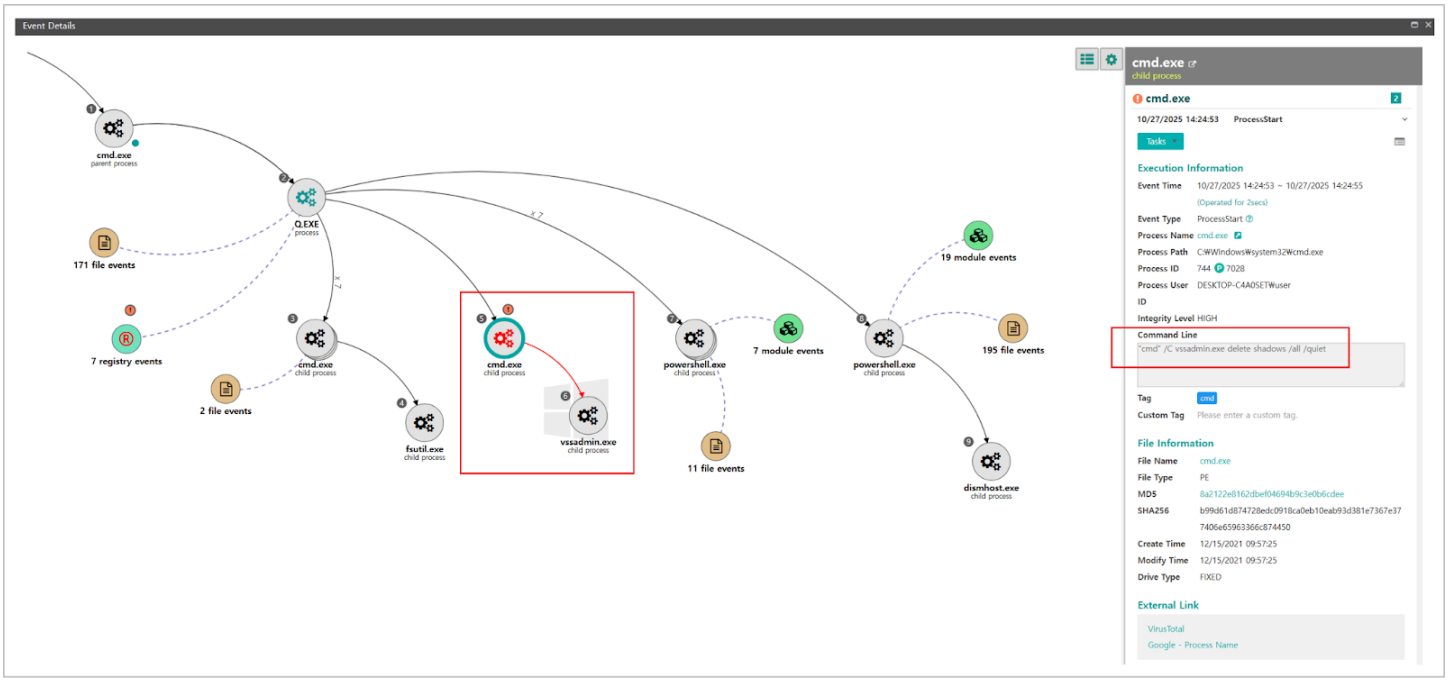
또한, 비정상적인 프로세스 행위, 파일 암호화 패턴 등 행위 기반(Behavior-based) 분석 기법을 적용하여, 기존에 알려지지 않은 신규 랜섬웨어(Unknown Ransomware) 역시 실시간으로 탐지 및 차단할 수 있습니다.



[사진 4-1] Genian EDR에서 Qilin 랜섬웨어 탐지 내역

Genian EDR은 랜섬웨어 실행 시 발생하는 VSS(Volume Shadow Copy Service) 삭제 명령을 실시간으로 모니터링 및 탐지하며, 정책 기반 대응 메커니즘에 따라 해당 악성 프로세스를 즉시 강제 종료(terminate)하여 추가적인 암호화 행위 및 시스템 손상을 차단합니다.

또한, 프로세스 트리(Process Tree) 및 이벤트 상관 관계 분석(Behavior Correlation Analysis)을 통해 공격 전·후 행위 전반에 대한 고가시성(High Visibility) 분석 화면을 제공함으로써, EDR 관리자가 위협 원인 및 영향 범위를 신속히 파악하고 대응할 수 있도록 지원합니다.



[사진 4-2] Genian EDR 이벤트 상세 그래프 화면

랜섬웨어 공격은 단순한 악성코드 감염을 넘어, 업무 마비와 데이터 손실, 금전적 피해를 초래하는 심각한 위협으로 자리 잡고 있습니다. 이러한 공격에 효과적으로 대응하기 위해 Genian EDR(Endpoint Detection and Response) 제품에는 Anti-Ransom 기능이 포함되어 있습니다. Anti-Ransom 기능은 일반적인 악성코드 탐지와 달리, 랜섬웨어의 특성을 기반으로 한 선제적 방어와 신속한 대응을 지원합니다.

Anti-Ransom 기능은 크게 세 가지 핵심 단계로 운영됩니다. 첫 번째는 행위 기반 탐지(Behavioral Detection)입니다. 랜섬웨어는 일반적으로 파일을 연속적으로 암호화하거나 확장자를 변경하는 등의 특이한 행동을 보이는데, Anti-Ransom 기능은 이러한 행위를 실시간으로 모니터링하여 감염 초기 단계에서 공격을 차단합니다. 이를 통해 파일이 완전히 암호화되기 전에 위협을 차단할 수 있습니다.

두 번째는 자동 격리 및 차단(Containment & Blocking) 단계입니다. Anti-Ransom 기능은 탐지된 프로세스를 자동으로 격리하거나 종료시키고, 추가적인 파일 암호화 시도를 즉시 차단합니다. 동시에 감염된 파일을 안전한 상태로 복원하거나 백업된 데이터를 활용해 신속히 복구할 수 있도록 지원함으로써, 업무 연속성을 최대한 보장합니다.

세 번째는 포렌식 및 대응 안내(Forensic Analysis & Response Guidance) 단계입니다. EDR 제품은 탐지된 랜섬웨어 공격의 상세 로그와 행위 데이터를 제공하며, 관리자에게 단계별 대응 절차를 안내합니다. 예를 들어, 감염 범위 확인, 격리 조치, 백업 파일을 통한 복원, 공격자 통신 차단 등 구체적인 대응 방법이 포함됩니다. 또한, 반복적 공격을 예방하기 위해 시스템 취약점 점검과 보안 정책 강화까지 권고 사항을 제공합니다.

결론적으로, EDR 제품의 Anti-Ransom 기능은 사전 예방, 실시간 차단, 빠른 복구, 체계적 대응 안내를 통합하여 랜섬웨어 공격에 대한 기업의 대응 능력을 크게 향상시킵니다. 단순히 감염 여부를 탐지하는 것에 그치지 않고, 실제 공격 상황에서 사용자가 즉시 취할 수 있는 단계별 지침을 제공함으로써, 피해를 최소화하고 신속한 업무 정상화를 가능하게 합니다.

5. IoC (Indicator of Compromise)

- **MD5**

1410b418a078559581725d14fa389cdd

440810b008eed766f085b69b1723f54b

a7ab0969bf6641cd0c7228ae95f6d217

a42d36f1af2c396e645ffa356fa47a1e

d0a711e4a51891ddf00f704d508b1ef2

d67303ba66bcb4dd89de87c83f3f831f

e1d41939dc4cc4116cc3439a01cfb666

e01776ec67b9f1ae780c3e24ecc4bf06

eb6fff4ee0f03ae5191f11570ff221c5

6b7eeb860917aa44982d8bd2d971aff1

14dec91fdcaab96f51382a43adb84016

31edb01d243e8d989eb7e5aeeeef54dc

63b89a42c39b2b56aae433712f96f619

64ca549e78ad1bd3a4bd2834b0f81080

88bb86494cb9411a9692f9c8e67ed32c

417ad60624345ef85e648038e18902ab

470d0261d18ed69990ce94f05d940de1

923c5af6fd29158b757fb876979d250b

0d68a310f4265821900249bec89364c2

0d70b3825647082d779987f2772bd219

08a2405cd32f044a69737e77454ee2da

11d795baafa44b73766e850d13b8e254

119856ec134acc86ef76044cbf291f54

지니언스㈜

대표이사: 이동범 | 사업자등록번호: 129-81-80148
경기도 안양시 동안구 벌말로 66 하이필드 지식산업센터 A동 12층
T. 031-8084-9770 | F. 070-4332-1683

문의 하기

제품 문의 바로가기
연동 문의 바로가기

FAMILY SITE

- FAMILY SITE
- Genians USA
- Genians Japan
- My Genians
- Partner portal
- Genians career