Keep up with Ransomware

지속적으로 리브랜딩되는 Global 랜섬웨어

■ 개요

2026 년 1 월 랜섬웨어 피해 사례 수는 지난 12 월(854 건) 대비 소폭 감소한 850 건으로 집계됐다.

2026 년 1 월 9 일, 대표적 해킹 포럼 중 하나인 BreachForums 의 사용자 데이터베이스가 유출됐다. James 라는 이름의 공격자는 ShinyHunter 의 사이트에 BreachForums 데이터베이스가 포함된 압축 파일과 장문의 선언문을 게시했다. 선언문에는 침해 사실을 입증하는 기술적 근거를 체계적으로 제시하기보다는 개인 서사와 명분 제시에 초점이 맞춰져 있으며 자기 과시적 서술과 표현이 다수 포함돼 있다. 그는 포럼 운영진과 관련 인물들을 실명 또는 별칭으로 거론하며 갈등 구도를 부각했다. 또한 프랑스를 겨냥한 공격이 발생했다는 점을 폭로의 결정적 계기로 제시하며, 이번 행위가 프랑스를 보호하기 위한 조치라는 취지로 주장했다. 다만 해당 선언문은 객관적 침해 증거 제시 없이 개인적 서사와 상징적 표현 위주로 구성돼 있어, 사실관계 검증이 어려운 내용이 다수 포함된 것으로 보인다. 이에 따라 정보의 신뢰성은 제한적일 것이라는 평가다.

한편, 2026 년 1 월 말에는 또 다른 해킹 포럼인 RAMP 가 법 집행기관에 의해 폐쇄된 것으로 확인됐다. RAMP 는 다크웹 해킹 포럼 중에서도 랜섬웨어 관련 홍보와 계열사 모집 활동을 허가한 곳으로 알려져 있다. 폐쇄 이후 사이트에는 FBI 압수 배너가 표시됐고, 배너에는 미 법무부 산하 CCIPS[1] 와 미국 플로리다 남부 연방검찰청의 공조가 명시됐다. 또한 운영자로 알려진 Stallman 은 수사기관이 RAMP 를 장악했다는 취지의 글을 XSS 포럼에 게시했다. 이어, 새 포럼 개설 계획은 없다고 덧붙였다.

1 월에는 국내 침해 사례가 여러 건 확인됐다. Qilin 그룹은 1 월 15 일 국내 제조업체를 공격해 회사 내부 자료와 비밀유지 계약서 등을 탈취했다고 주장하며, 이를 다크웹 유출 사이트에 게시했다. 또한 1 월 30 일 Qilin 그룹은 국내 공영 방송사를 피해자로 지목했지만, 샘플 데이터가 공개되지 않아 실제 침해 및 데이터 탈취 여부는 확인되지 않았다.

[1] CCIPS(Computer Crime and Intellectual Property Section): 미국 법무부 형사국 산하로, 컴퓨터 범죄 및 지식재산 관련 수사·기소 지원과 전자 증거 수집 자문 등을 담당하는 조직

■ 랜섬웨어 뉴스

BreachForums 데이터베이스 유출

- James라는 이름의 공격자가 ShinyHunters 사이트에 BreachForums 데이터베이스 압축 파일과 장문의 선언문을 공개
- 선언문은 기술적 근거보다 개인 서사와 명분 주장에 치우쳤고 관련 인물을 실명 또는 별칭으로 거론
- 객관적 침해 증거가 부족하고 사실관계 검증이 어려운 내용이 많아 정보 신뢰성은 낮은 것으로 판단

RAMP 포럼 법 집행기관 공조로 폐쇄

- 2026년 1월 말, 해킹 포럼 RAMP가 법 집행기관에 의해 폐쇄된 것으로 확인됐으며 사이트에 FBI 압수 배너가 표시
- RAMP는 랜섬웨어 홍보 및 계열사 모집을 허용해온 다크웹 해킹 포럼으로 알려짐
- 운영자는 XSS 포럼에 법 집행기관이 RAMP를 장악했다는 취지의 글을 올렸으며 새 포럼을 개설할 계획은 없다고 밝힘

Qilin 그룹 국내 기업 2곳 공격

- 국내 제조업체를 공격해 내부 자료 등을 탈취했다고 주장하며 다크웹 유출 사이트에 게시
- 국내 방송사를 피해자로 다크웹 유출 사이트에 게시하고 업종을 광고 마케팅으로 표기
- 방송사 공격 건은 샘플 데이터가 공개되지 않아 실제 침해 및 데이터 탈취 여부가 확인되지 않음

2026년 1월 신생 그룹 8개 등장

- 12월에 등장한 신규 랜섬웨어 그룹 7곳은 자체 다크웹 유출 사이트를 운영
- 다크웹 유출 사이트를 운영하는 그룹 중 Vect의 다크웹 유출 사이트는 비활성화된 상태로 확인

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

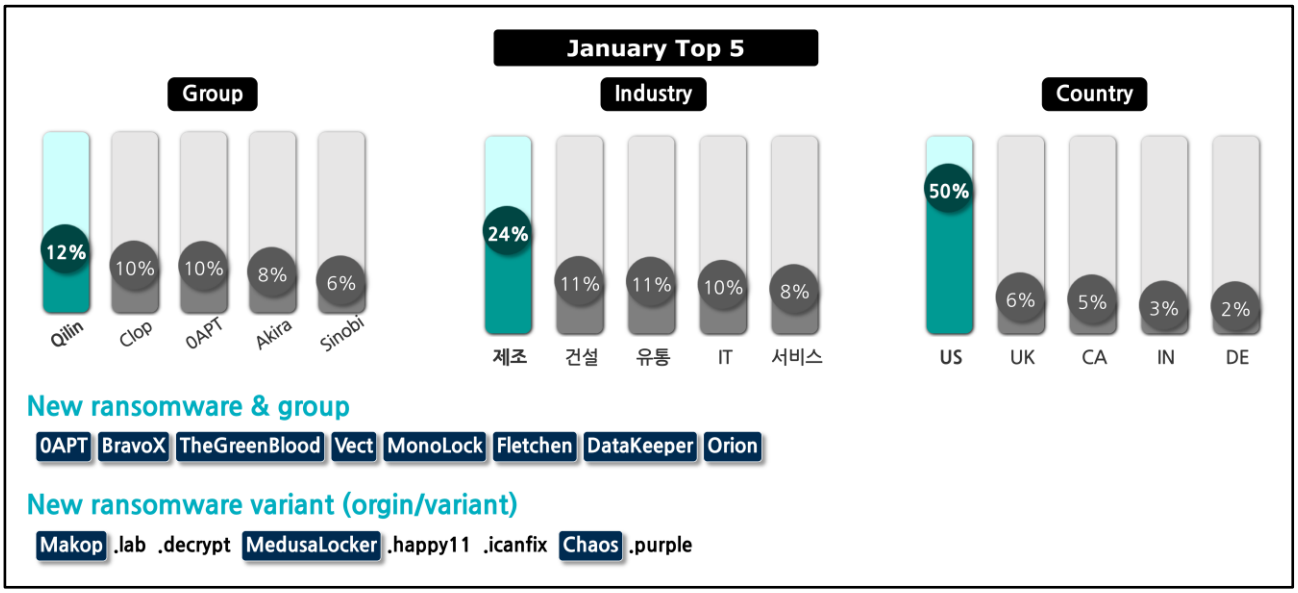


그림 2. 2026 년 1 월 랜섬웨어 위협 현황

새로운 위협

2026 년 1 월에는 신규 랜섬웨어 그룹 8 개가 등장했다. 이 중 0APT, BravoX, TheGreenBlood, Vect, Fletchen, DataKeeper, Orion 은 다크웹 유출 사이트를 보유하고 있으나 현재 Vect 의 다크웹 유출 사이트는 비활성화된 상태로 확인된다.

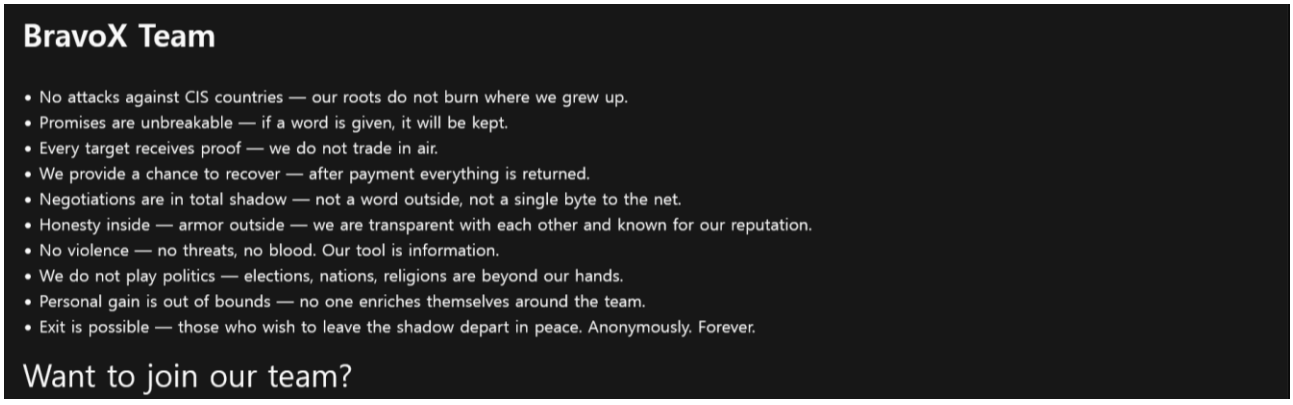


그림 3. BravoX 그룹의 RaaS[2] 모집글

[2] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 쉽게 랜섬웨어를 만들고 공격할 수 있도록하는 비즈니스모델

2026 년 1 월에 등장한 BravoX 그룹은 현재까지 총 3 건의 피해자를 게시했다. 이들은 RaaS 계열사 모집 글에서 CIS[3] 국가를 공격 대상에서 제외한다고 밝히는 한편, 침투 테스트 경험을 보유하고 공격 목표가 명확한 계열사를 모집한다고 강조했다. 또한 계열사 가입 조건으로 연 매출 500 만 달러(한화 약 73 억) 이상 기업을 대상으로 유출한 미공개 데이터 제출, Exploit[4] 포럼에 5,000 달러(한화 약 729 만원) 보증금 예치, 기존 계열사 또는 기존 멤버 추천 등 3 가지 조건 중 최소 1 가지를 충족할 것을 제시했다.

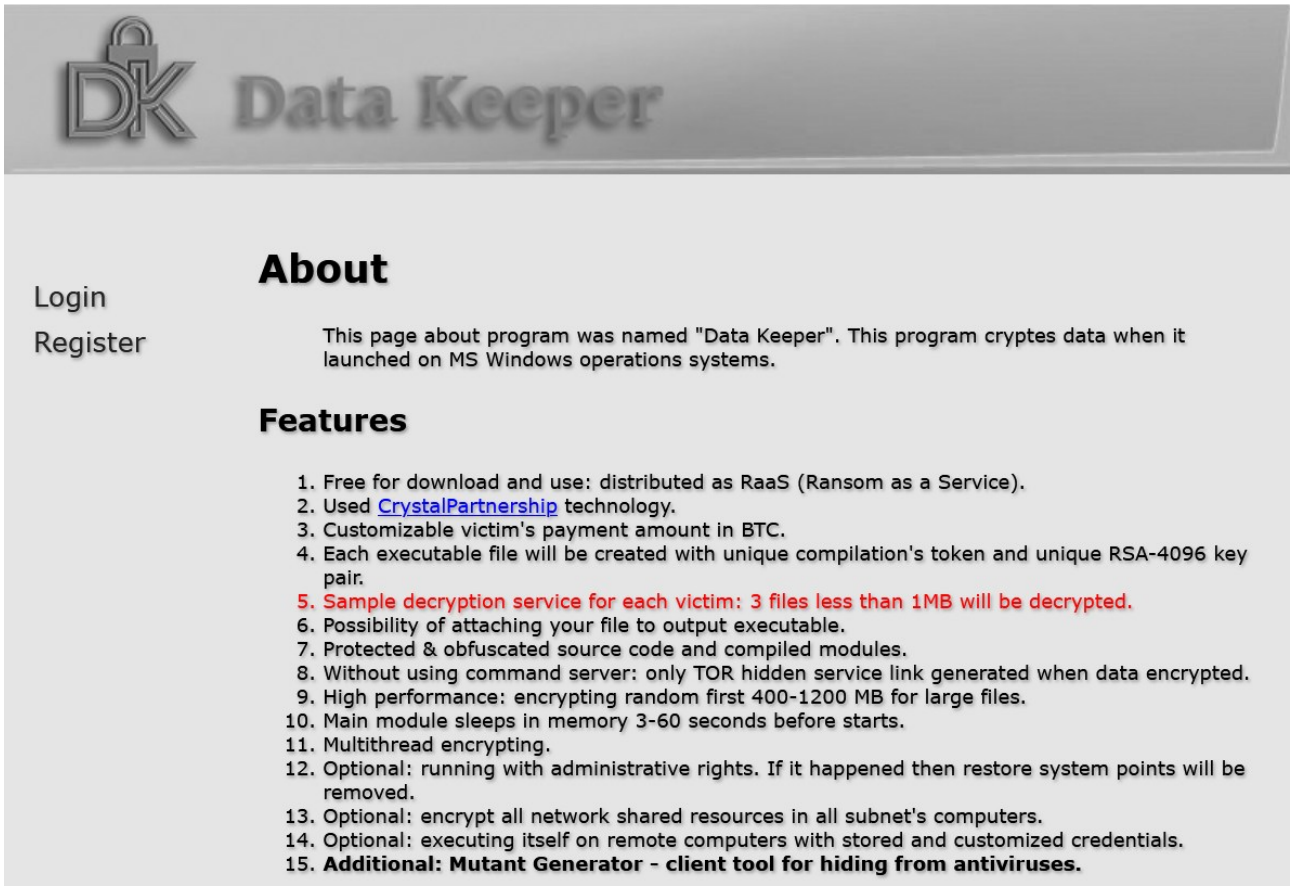


그림 4. DataKeeper 그룹의 RaaS 모집글

2026 년 1 월 처음 확인된 DataKeeper 그룹은 RaaS 계열사 모집 글에서 기존과 차별화된 수익 정산 시스템을 내세우고 있다. 일반적인 RaaS 정산 구조는 피해자 지불금이 운영자 지갑으로 유입된 뒤, 운영자가 계열사 몫을 사후 배분하는 방식이 많아 정산 지연이나 미지급 등 문제가 발생할 수 있다. 반면 DataKeeper 는 피해자 지불 단계에서 운영자와 계열사 지갑으로 수익이 자동 분할되어 배분되는 정산 구조를 표방해 계열사가 운영자의 정산 절차에 의존하지 않는 분배 모델을 강조한다.

[3] CIS(Commonwealth of Independent States): 구 소련권 국가들을 중심으로 구성된 지역 협의체

[4] Exploit: 러시아 해킹 포럼으로, 취약점 및 초기 침투 접근 권한 등이 거래되는 곳

Top5 랜섬웨어

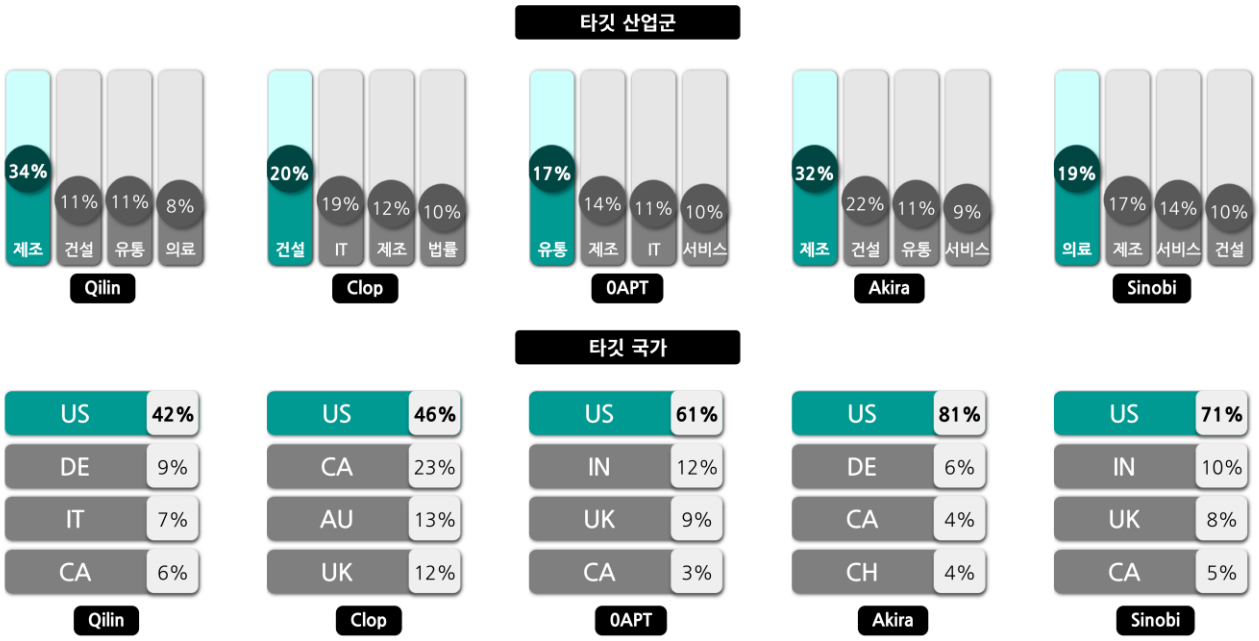


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

2026 년 1 월 기준 가장 많은 피해를 발생시킨 랜섬웨어 그룹은 Qilin 으로, 한 달 동안 총 108 건의 피해를 일으킨 것으로 확인됐다. 또한 Qilin 은 1 월 12 일 캐나다의 건설사 Pre-Con Builders 를 공격해 515GB 규모의 데이터를 탈취했다고 주장하며, 관련 내용을 다크웹 유출 사이트에 게시했다.

지난 2025 년 11 월 Oracle E-Business Suite 의 취약점(CVE-2025-61882)을 악용해 2025 년 11 월 97 건의 피해자를 다크웹 유출 사이트에 공개하며 활동이 급증했던 Clop 그룹은 2026 년 1 월 91 건의 피해자를 발생시켰다. Qilin 다음으로 두 번째로 많은 피해 사례를 기록했다.

0APT 그룹은 2026 년 1 월 등장 직후 단기간에 다크웹 유출 사이트에 약 90 건의 피해자 목록을 게시했다. 다만 다수의 항목은 샘플 파일이나 침해 증거 없이 등록됐고, 협상 마감 기한이 지난 항목에도 데이터가 공개되지 않는 등 피해 주장에 대한 검증 요소가 확인되지 않았다. 또한 실제로 존재하지 않는 기업을 피해자로 올린 정황도 확인돼 주장에 대한 신빙성이 낮은 것으로 판단된다.

Akira 그룹은 2026 년 1 월 피해 76 건을 발생시키며, 1 월 기준 네 번째로 많은 피해 사례를 기록한 것으로 확인됐다. Akira 그룹은 1 월 29 일 미국의 마케팅 기업 Crosslists Data 를 공격해 직원 개인정보와 계약서 등이 포함된 약 21GB 규모의 데이터를 탈취한 뒤, 이를 다크웹 유출 사이트에 공개하겠다고 협박했다.

Sinobi 그룹은 2026 년 1 월 27 일 미국의 비영리 기관 Affordable Housing Management Overview Metrics 를 공격해 재무 데이터와 고객 정보 등이 포함된 약 50GB 크기의 데이터를 탈취한 뒤 500 만 달러(한화 약 73 억 원)를 요구했다.

■ 랜섬웨어 집중 포커스

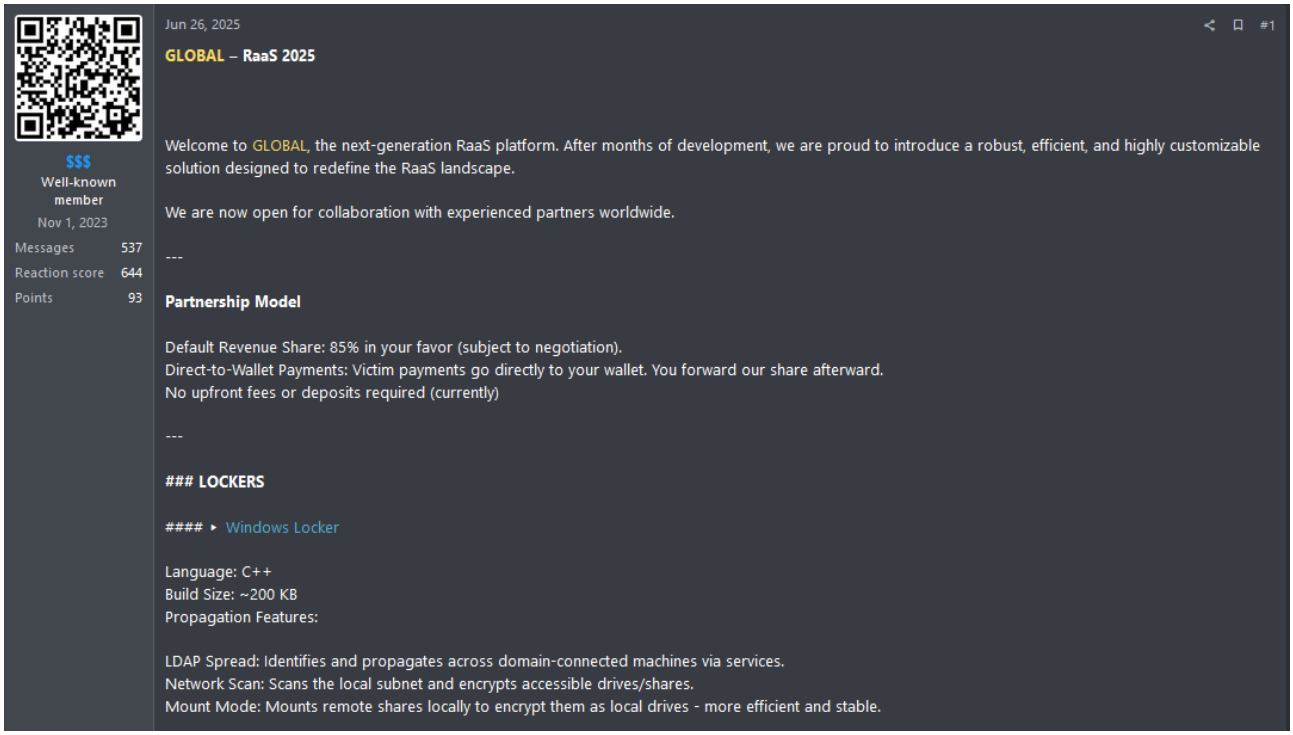


그림 6. Global 랜섬웨어 그룹의 RaaS 홍보글

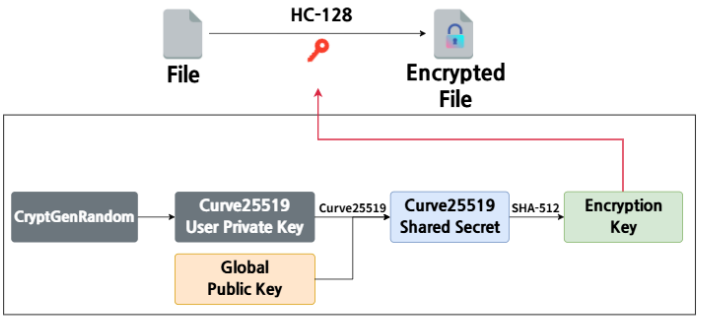
Global 랜섬웨어는 2025 년 6 월에 등장했다. Mamona 랜섬웨어 그룹의 리브랜딩으로 추정되는 정황이 포착됐다. Global 은 기존 Mamona 랜섬웨어와 매우 유사하며, 비교 분석 결과 일부 기능이 추가된 버전으로 확인됐다. 또한 Global 의 랜섬노트에는 Mamona 그룹의 운영자가 관여한 또 다른 프로젝트로 알려진 BlackLock 그룹의 다크웹 유출 사이트 주소가 포함되어 있었다.

아울러 운영진으로 알려진 "$$$"는 러시아 해킹 포럼 RAMP 에서 프로필과 홍보 게시물의 표기를 "Global BlackLock"으로 변경했으며, 2025 년 6 월 말에는 Global RaaS 를 홍보하는 게시물을 추가로 게시했다. 이러한 정황은 두 프로젝트 간 연계를 뒷받침한다.

또한 Global 의 최신 샘플 랜섬노트에 Aware 그룹의 협상 주소가 포함된 정황을 고려하면, Global 이 Aware 로 추가 리브랜딩 됐을 가능성도 제기된다. 이러한 정황을 종합하면 Mamona → Global → Aware 로 이어지는 흐름은 연속적인 리브랜딩으로 볼 수 있다. 이에 본 보고서는 향후 위협에 대비할 수 있도록 그룹 간 연계 정황을 종합하고, Global 랜섬웨어의 상세 분석 결과를 공유하고자 한다.

암호화 키

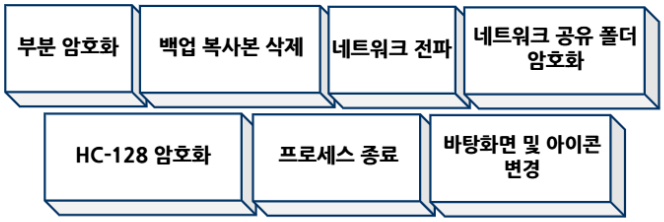
Curve25519 알고리즘으로 암호화 키를 생성하며 HC-128 알고리즘으로 암호화



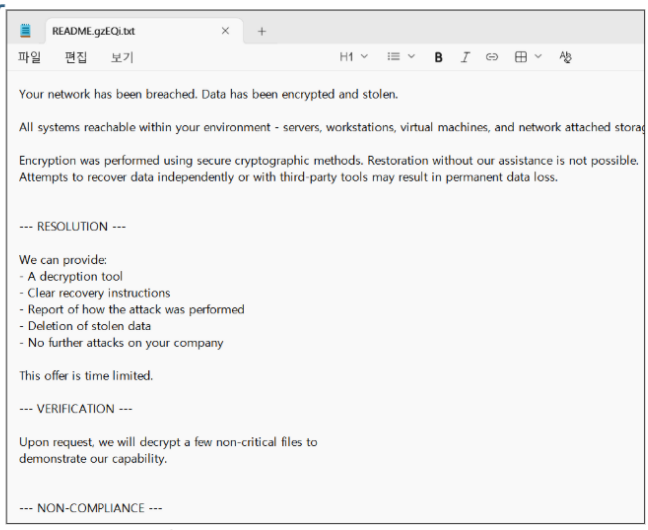
암호화 방식

* 암호화 방식 1.
1MB 이하: 전체 암호화
1MB 초과 5MB 이하: 파일의 첫 1MB 암호화
5MB 초과: 파일의 처음부터 파일 전체 크기의 N% 만큼 암호화(최대 70MB)
* 암호화 방식 2.
64Bytes 이하: 전체 암호화
64Bytes 초과 5MB 이하: 파일의 처음부터 전체 크기의 10%만큼 암호화
5MB 초과 20MB 이하: 파일 크기의 1/6 마다 첫 4KB 암호화
20MB 초과: 10MB 마다 첫 4KB 암호화

특징



랜섬노트


README.gzEQi.txt

파일 편집 보기

Your network has been breached. Data has been encrypted and stolen.

All systems reachable within your environment - servers, workstations, virtual machines, and network attached storag

Encryption was performed using secure cryptographic methods. Restoration without our assistance is not possible.
Attempts to recover data independently or with third-party tools may result in permanent data loss.

--- RESOLUTION ---

We can provide:
- A decryption tool
- Clear recovery instructions
- Report of how the attack was performed
- Deletion of stolen data
- No further attacks on your company

This offer is time limited.

--- VERIFICATION ---

Upon request, we will decrypt a few non-critical files to
demonstrate our capability.

--- NON-COMPLIANCE ---

README.gzEQi.txt

변경 확장자

.gzEQi

제작 언어

C/C++

그림 7. Global 랜섬웨어 개요

랜섬웨어 전략

그림 8. 랜섬웨어 공격 전략

Global 랜섬웨어는 Mamona 랜섬웨어와 동일하게 다양한 실행 인자를 사용해 암호화 동작을 정밀하게 제어할 수 있도록 설계되어 있으며, 사용되는 인자와 기능은 아래 표와 같다.

인자	설명
-log	로그 출력
-keep	자가 삭제 비활성화
-skip-net	로컬 디스크만 암호화
-skip-local	네트워크만 암호화
-code {32bytes key}	랜섬웨어 실행에 필요한 비밀번호
-sub {subnet}	네트워크 암호화 대상 네트워크 대역
-p {password}	네트워크 로그인 비밀번호
-u {username}	네트워크 로그인 이름
-time {HH:MM}	지정한 시각까지 대기 후 실행
-delay {ss}	지정한 시간동안 대기 후 실행
-threads {int}	암호화 스레드 수 설정
-path {path}	특정 폴더 암호화
-host {ip_addr}	특정 호스트 암호화
-ldap	네트워크 전파 암호화
-detached	랜섬웨어 재실행 비활성화

표 1. 랜섬웨어 실행인자

Global 랜섬웨어의 인자는 Mamona 랜섬웨어와 대부분 동일하다. 차이점이 있다면 Mamona 버전에서는 네트워크 인증을 위해서 NTLM[5] 해시를 전달할 때 사용하던 -H 인자가 Global 랜섬웨어에서는 삭제됐다. 또한 네트워크 전파 활성화를 위한 -ldap 인자와 네트워크 전파 대상을 지정하기 위한 –host 인자, 디버거 분리 기능을 비활성화하기 위한 -detached 인자가 함께 추가됐다.

Global 랜섬웨어는 실행 시 중복 실행을 방지하기 위해 Global\\Fxo16jmdgujs437 문자열을 사용해 뮤텍스[6] 를 생성한다. 해당 뮤텍스 문자열은 Mamona 랜섬웨어가 뮤텍스를 생성할 때 사용하는 문자열과 동일하다.

이후 Global 랜섬웨어는 Mamona 랜섬웨어와 동일한 방식으로 복구 방지와 분석 방해를 위해 각종 기록이나 흔적을 삭제한다. 휴지통에 있는 데이터를 모두 삭제하며, 시스템의 모든 이벤트 로그를 삭제한다.

[5] NTLM: 보안 인증 프로토콜 중 하나로, 인증을 위해 실제 암호 대신 해시를 전달해 권한 부여 및 인증을 제공하는 기능

[6] 뮤텍스(Mutex): 하나의 자원에 여러 스레드 혹은 프로세스가 동시에 접근하지 못하도록 하는 동기화 매커니즘으로, 랜섬웨어에서는 흔히 중복 실행 방지를 위해 사용한다

또한 암호화된 파일을 사용자가 임의로 복구하지 못하도록 명령 프롬프트 명령어를 활용해 백업 복사본을 삭제한다. 백업 복사본을 삭제하기 위해 사용하는 명령어는 아래와 같다.

백업 복사본 삭제 명령어
cmd.exe /c vssadmin delete shadows /all /quiet

이후 원활한 파일 암호화를 위해 특정 서비스와 프로세스를 종료한다. 이때 종료 대상은 Mamona 버전 대비 종료 대상이 추가됐으며, 상세 목록은 아래 표와 같다.

서비스	프로세스
WinDefend, SecurityHealthService, wscsvc, Sense, WdNisSvc, WdNisDrv, WdFilter, WdBoot, wdnisdrv, wdfilter, wdboot, mpssvc, mpsdrv, BFE, MsMpSvc, SepMasterService, wscsvc, SgrmBroker, SgrmAgent, EventLog, SepMasterService, MBAMService, MSSQLSERVER, SQLSERVERAGENT, SQLBrowser, MSSQL$SQLEXPRESS, SQLAgent$SQLEXPRESS, OracleServiceXE, OracleXETNSListener, OracleJobSchedulerXE, MySQL, MySQL80, PostgreSQL	MsMpEng.exe, NisSrv.exe, SecurityHealthService.exe, smartscreen.exe, SecHealthUI.exe, MpCmdRun.exe, MSASCui.exe, MpUXSrv.exe, SgrmBroker.exe, MsSense.exe, SenseIR.exe, SenseCE.exe, SenseSampleUploader.exe, SenseNdr.exe, SenseCncProxy.exe, sqlservr.exe, sqlbrowser.exe, oracle.exe, tnslsnr.exe, mysqld.exe, postgres.exe, pg_ctl.exe, mongodb.exe, mongod.exe

표 2. 종료 대상 서비스 및 프로세스

암호화 설정은 실행 인자에 따라 구분된다. -skip-local 을 사용하면 네트워크 공유 폴더만 암호화하며, -skip-net 을 사용하면 로컬 디스크만 암호화한다. 또한 -path 인자를 지정하면 특정 디렉토리와 그 하위 디렉토리만 대상으로 암호화를 수행한다. 암호화 대상을 설정한 뒤에는 각 디렉터리를 순회하면서, 파일이 예외 항목에 해당하는지 여부를 확인한다. Global 버전은 예외 확장자 목록에 .bin 이 추가된 것을 제외하면 Mamona 랜섬웨어와 동일하며, 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
Windows, Program Files, Program Files (x86), AppData, ProgramData, All Users, NETLOGON, SYSVOL	PrintMe22.pdf, .exe, .dll, .msi, .sys, .ini, .ink, .bin

표 3. 암호화 예외 대상

Global 랜섬웨어는 로컬 시스템뿐만 아니라 네트워크 환경으로도 전파된다. 해당 기능은 -ldap 인자를 지정해야 활성화되며, -host 로 전파 대상을 특정 호스트로 제한하거나 -sub 로 특정 서브넷 대역 전체로 확장할 수 있다.

Global 랜섬웨어는 LDAP[7] 을 활용해 전파하는 방식을 사용한다. -u 인자로 전달받은 로그인 아이디가 id@domain 형태인 경우, 해당 문자열에서 도메인 정보를 추출해 사용하며 추출한 정보를 기반으로 AD[8] 에 연결된 모든 시스템 정보를 수집한다. 이후 각 시스템에 대해 -u 인자의 계정과 -p 인자의 비밀번호로 인증 가능 여부를 확인하고, 인증이 성공한 시스템에 랜섬웨어를 전파한다.

반면 Mamona 랜섬웨어는 전파 과정에서 IPC$[9] 를 통해 네트워크 연결을 시도한다. 이때 -u, -H, -p 인자를 통해 각각 로그인 아이디, 인증용 NTLM 해시, 로그인 비밀번호를 입력 받지만, -H 로 해시 값을 전달받더라도 실제 NTLM 해시 기반 인증은 수행하지 않는다. 대신 -u 와 -p 조합으로 로그인을 시도하며, 접속이 가능한 경우 별도의 랜섬웨어 전파 없이 해당 네트워크 공유 자원 내 파일을 암호화하는 방식으로 동작한다.

```
sprintf_s_0(Name, 0x104u, L"\\\\%s\\admin$", WideCharStr);
GetModuleFileNameW(0, Filename, 0x104u);
sprintf_s_0(NewFileName, 0x104u, L"%s\\Temp\\cleanup.exe", Name);
NetResource.dwType = 1;
NetResource.dwScope = 0;
memset(&NetResource.dwDisplayType, 0, 12);
NetResource.lpComment = 0;
NetResource.lpProvider = 0;
NetResource.lpRemoteName = Name;
if ( byte_4390C4 )
  _printf_p("[+] Connecting to share: %ws\n", Name);
v6 = WNetAddConnection2W(&NetResource, lpPassword, lpUserName, 0);
if ( v6 )
{
  if ( byte_4390C4 )
    _printf_p("[!] Failed to connect to share: %ws (Error: %d)\n", Name, v6);
  return 0;
```

그림 9. 랜섬웨어 전파 및 실행

[7] LDAP: 네트워크 상에서 사용자, 그룹, 장비, 인증 정보 등의 데이터를 저장하고 조회 가능하게 하는 프로토콜

[8] AD (Active Directory): LDAP 기반의 Windows 통합 디렉터리 시스템으로 사용자와 컴퓨터를 일괄적으로 관리 가능

[9] IPC$: 네트워크를 통해 다른 컴퓨터에 접근하려 할 때, 인증을 수행하기 위한 제어용 공유 폴더

연결된 시스템의 임시 디렉토리에 랜섬웨어를 cleanup.exe 파일명으로 복사한 뒤, 서비스 등록 또는 작업 스케줄러 등록 방식으로 실행한다. 또한 동일 네트워크 내에서 전파가 반복 시도되는 상황을 막기 위해 원격 호스트에서는 실행 시 -skip-net 인자를 추가한다. 관련 실행 명령은 아래 표와 같다.

원격 호스트 서비스 생성
sc \\{host_ip} create Radio_[0-9]{32} binPath= "%%windir%%\\Temp\\cleanup.exe -skip-net" start= demand

작업 스케줄러 작업 생성
schtasks /create /s {host_ip} /u {username} /p {password} /tn "CoolTask" /tr "%%windir%%\Temp\cleanup.exe -skip-net" /sc once /st 00:00

서비스 실행
sc \\{host_ip} start Radio_[0-9]{32}

작업 스케줄러 작업 실행
schtasks /run /s {host_ip} /u {username} /p {password} /tn

작업 스케줄러 작업 삭제
schtasks /delete /s {host_ip} /u {username} /p {password} /tn

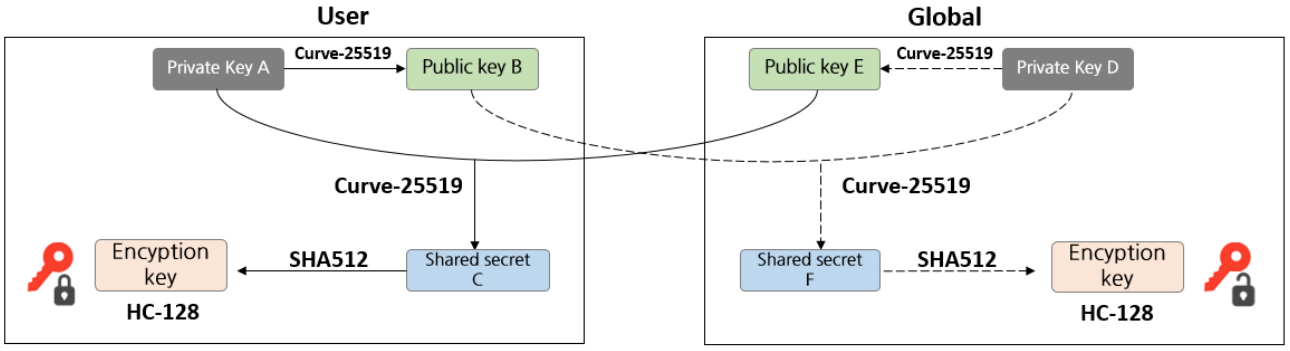


그림 10. 암호화 키 생성 방식

Global 랜섬웨어는 파일 암호화를 위해 파일마다 고유한 개인키(A)를 생성한다. 이후 하드코딩된 공격자의 공개키(B)와 Curve-25519 연산을 수행해 공유 비밀(C)을 만든다. 이때 공유 비밀이란, Curve25519 알고리즘에서 양측이 각자의 개인키와 상대방의 공개키만으로 동일하게 계산되는 값을 의미한다.

즉 피해자의 개인키(A)와 공격자의 공개키(B)로 계산한 값(C)은, 공격자의 개인키(D)와 피해자의 공개키(E)로 계산한 값(F)과 동일하며, 이 동일한 값(C, F)을 공유 비밀이라고 한다. 이때 생성된 공유 비밀은 바로 사용되지 않고 SHA-512 알고리즘으로 해시를 생성 후 뒤에서부터 32 바이트를 키로 이용해 HC-128 알고리즘으로 파일 암호화를 수행한다. 암호화가 완료되면 파일의 끝에 피해자의 공개키(E)를 저장한다. 공격자는 이 공개키(E)와 자신이 보유한 개인키(D)를 이용해 공유 비밀을 다시 계산할 수 있으며, 같은 방식으로 해시를 적용해 파생키를 생성함으로써 해당 파일을 복호화할 수 있다.

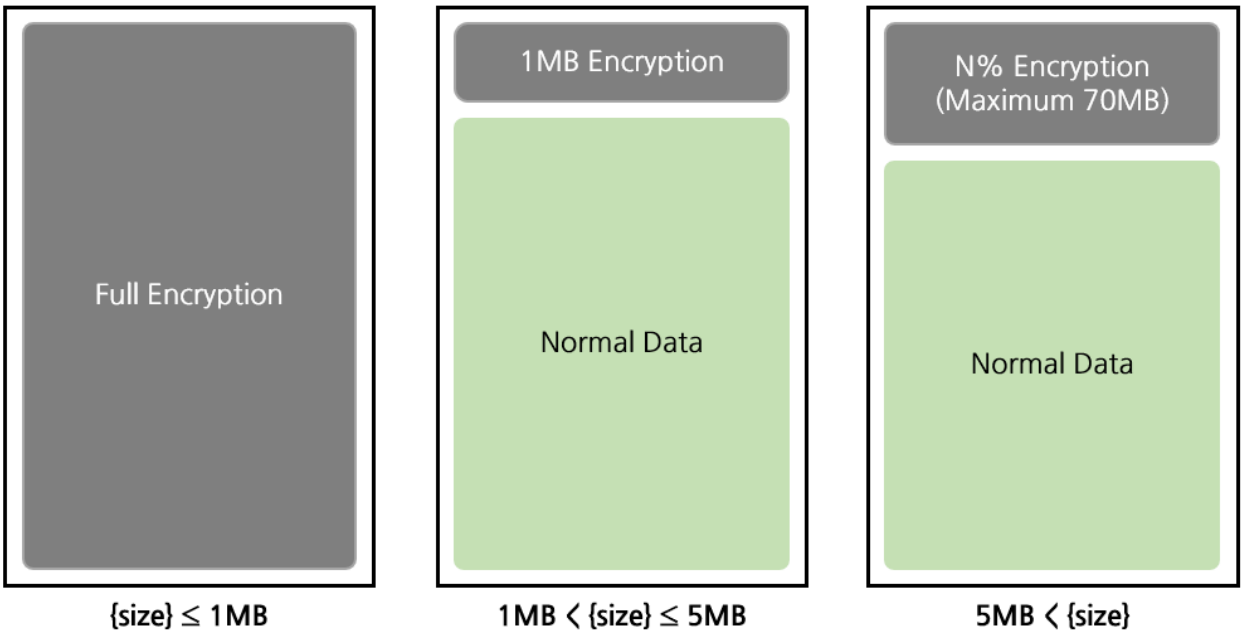


그림 11. 파일 암호화 방식(1)

파일 암호화 방식은 Mamona 랜섬웨어와 동일하게 두 가지 암호화 모드로 구분된다. 첫 번째 방식은 크기가 큰 파일의 경우 앞부분 일부만 암호화하는 방식이다. 1MB 이하의 파일은 전체 암호화를 진행하며, 5MB 이하의 파일은 처음 1MB 만큼만 암호화한다. 5MB 보다 큰 파일은 공격자가 지정한 비율만큼 파일의 첫 부분을 암호화하는데, 그 크기가 최대 70MB 로 제한되어 있다.

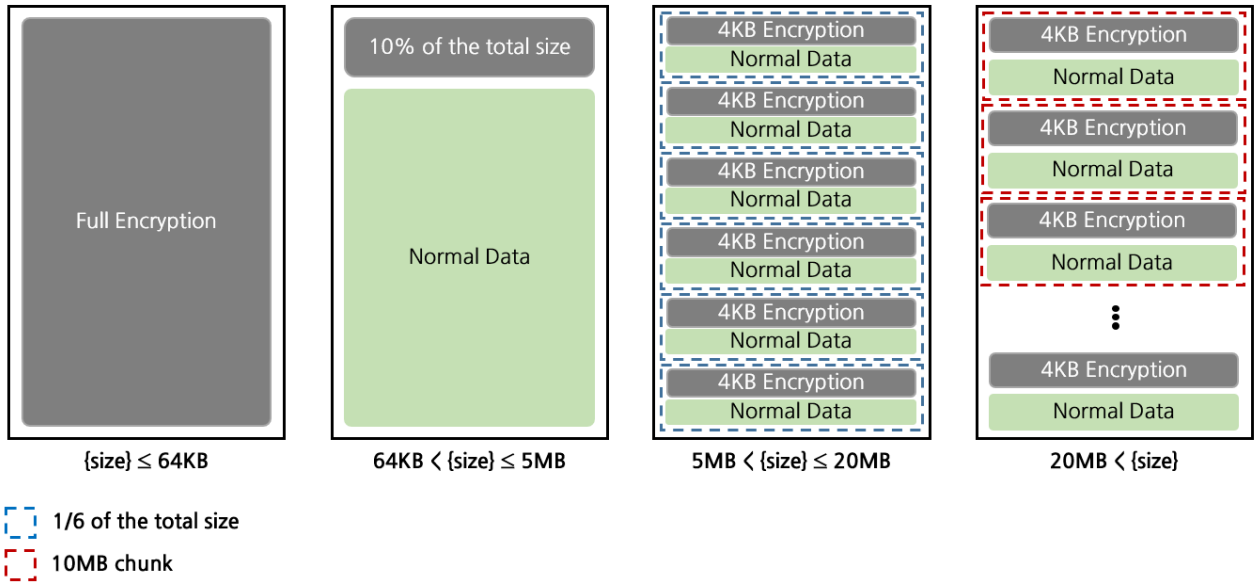


그림 12. 파일 암호화 방식(2)

두 번째 방식은 파일의 일정 간격마다 암호화하는 방식이다. 64Bytes 이하의 파일은 전체 암호화를 하며, 5MB 이하의 파일은 전체 크기의 10%만큼만 암호화한다. 20MB 이하의 파일은 전체 크기의 1/6 만큼 구간을 나누어 각 구간의 첫 4KB 만 암호화하고, 20MB 보다 큰 파일은 10MB 마다 처음 4KB 를 암호화한다.

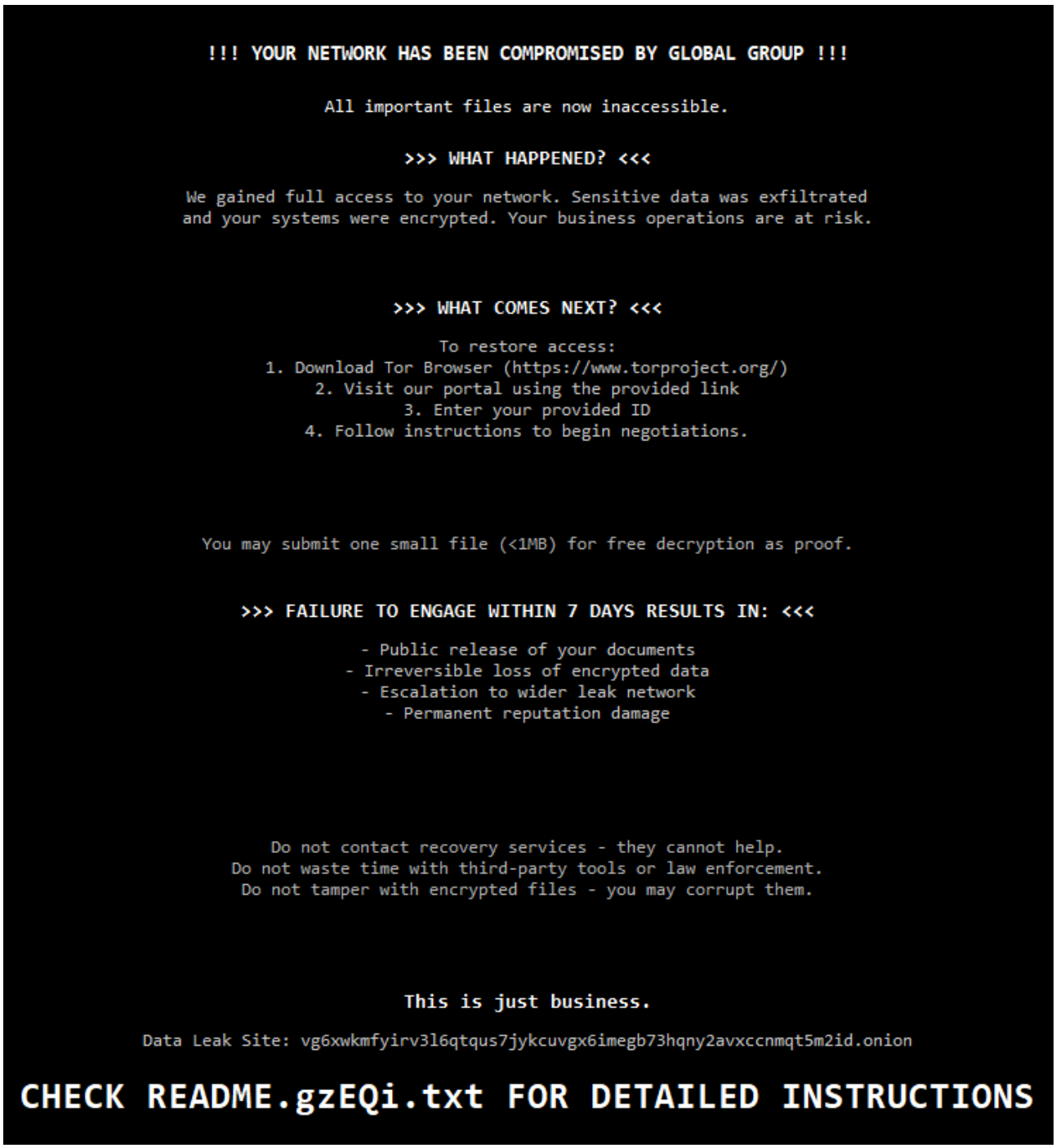


그림 13. 변경된 바탕화면

파일 암호화가 완료되면, 랜섬웨어는 실행 시점에 Global 감염 문구가 삽입된 바탕화면 이미지를 생성하고, 바탕화면을 해당 이미지로 변경한다. 이때 바탕화면에는 Global 랜섬웨어의 다크웹 유출 사이트 주소와 랜섬노트를 확인하라는 안내가 포함된다. 그러나 랜섬노트에 포함된 링크는 Global 이 아닌 Aware 그룹의 다크웹 사이트로 연결되는 것으로 확인되며, 이는 두 그룹 간 리브랜딩 또는 제휴 가능성을 시사한다.

모든 파일 암호화가 끝난 뒤에는 랜섬웨어를 자체적으로 삭제한다. 이때 사용되는 명령어는 아래와 같다.

랜섬웨어 자가 삭제 명령어
cmd.exe /C ping 127.0.0.7 -n 3 > Nul & Del /f /q \"%s\

랜섬웨어 대응방안

그림 14. 랜섬웨어 대응방안

Global 랜섬웨어는 파일 암호화 및 네트워크 전파 과정에서 네트워크 공유 폴더, 도메인 정보 등 다양한 시스템, 네트워크 정보를 활용한다. 따라서 행위 기반 솔루션을 적용해 관련 악성 행위를 조기에 차단하고, 불필요한 네트워크 서비스를 제거하거나 비활성화하여 네트워크를 통한 피해 확산을 억제할 필요가 있다.

또한 랜섬웨어는 네트워크 환경으로 전파하기 위해 로그인 ID 와 비밀번호를 이용해 원격 시스템 접근을 시도한다. 별도의 ID, 비밀번호 수집 행위는 확인되지 않았으나, 공격 준비 단계에서 계정 정보를 수집하거나 유출 계정 또는 취약한 계정을 악용할 가능성이 있다. 이러한 때는 2FA[10] 를 적용해 인증을 강화해야 한다. 더불어 원격 서비스 사용 계정을 최소화하고, 불필요한 원격 서비스는 비활성화하여 공격자가 네트워크 환경에 접근하기 어렵게 만들어야 한다.

[10] 2FA (2-factor Authentication): ID/PW 인증 외에도 휴대전화나 OTP 등을 활용한 추가 인증 수단으로 인증하는 방식

이와 함께 초기 침투 및 비정상 행위를 신속히 식별, 차단하기 위해 EDR 도입과 최신 보안 패치 적용이 필요하다. 아울러 백업 복사본은 별도의 네트워크 구간이나 외부 저장소, 오프라인 매체에 주기적으로 분산 백업하여 시스템이 암호화되더라도 데이터 복구가 가능하도록 대비해야 한다. 이때 백업 장치 접근 권한을 최소화하고, 정기적인 복구 테스트를 수행해 백업 데이터의 무결성을 지속적으로 검증해야 한다.

앞서 언급한 악성 행위는 주로 Windows 명령 프롬프트 기반 실행, 작업 스케줄러 등록, 서비스 등록 방식으로 수행된다. 따라서 ASR[11] 규칙을 활성화해 비정상 프로세스를 차단함으로써 악성 행위를 완화할 수 있다. 또한 랜섬웨어가 임시 폴더에 프로그램을 저장하거나 작업 등록을 위해 특정 경로로 랜섬웨어를 복제하는 특성이 있으므로 백신을 활용해 의심 파일을 격리하는 대응도 가능하다.

[11] ASR (Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

IoCs

Hash(SHA-256)
f6f7a37b49310287a253dbdf81e22f0593f44111215ca9308e46d2c68516196f

■ 참고 사이트

• Resecurity (https://www.resecurity.com/blog/article/doomsday-for-cybercriminals-data-breach-of-major-dark-web-foru)

• The Record (https://therecord.media/notorious-russia-based-ramp-forum-seized)