Yurei 랜섬웨어 Go 기반 빌더 암호화 구조 분석

asec.ahnlab.com/ko/90933

ATCP

November 10, 2025

Yurei 랜섬웨어 그룹은 2025년 9월 초 처음으로 공개적으로 확인된 신규 랜섬웨어 그룹이다. 해당 그룹은 기업 네트워크를 침입하여 데이터를 암호화하고, 백업을 삭제한 후, 탈취한 정보를 기반으로 이중 갈취 방식의 몸값을 요구하는 전형적인 랜섬웨어 운영 모델을 채택하고 있다. 현재까지 RaaS(서비스형 랜섬웨어) 또는 다른 그룹과의 협력 관계에 대한 명확한 증거는 발견되지 않았으며, 기존 랜섬웨어 그룹의 리브랜딩이나 변형에 대한 보고 역시 없는 상태이다. 피해자와의 접촉은 전용 다크웹 사이트를 통해 이루어진다.

확인된 피해 국가로는 스리랑카와 나이지리아가 있으며, 주요 표적 산업은 운송·물류, IT 소프트웨어, 마케팅·광고, 식품·외식업 등으로 파악된다. 복구를 위한 몸값은 피해 기업의 재정 상황을 조사한 후 개별적으로 산정되는 것으로 알려졌으나, 구체적인 요구 금액 범위에 대한 정보는 공개되지 않았다.

[그림 1] Yurei 랜섬웨어 DLS 사이트

분석 내용

Yurei 랜섬웨어는 Go 언어로 개발된 랜섬웨어로, 일반적인 랜섬웨어의 권한 변경, 인자 값 설정, Mutex 생성, 문자열 복호화 등의 특별한 초기 루틴 없이 바로 암호화 준비 루틴을 수행한다. 파일 암호화에는 ChaCha20-Poly1305 알고리즘을 사용하며, 32 Byte Key와 24 Byte Nonce를 랜덤 값으로 생성한다. 생성된 Key와 Nonce는 내장된 Public Key를 사용하여 secp256k1-ECIES 방식으로 암호화하며, 암호화된 파일 내부에 함께 저장된다. 즉, 대응되는 secp256k1-ECIES Private Key를 가진 공격자만 복호화 할 수 있도록 설계되어 있다.

암호화 준비

Yurei 랜섬웨어는 일반적인 랜섬웨어의 권한 변경, 인자 값 설정, Mutex 생성, 문자열 복호화 등의 특별한 초기 루틴 없이 바로 암호화 준비 루틴을 수행한다. 암호화를 수행하기 위해 현재 실행 환경의 드라이브 정보를 얻으며, 모든 드라이브 경로를 순회하며 암호화 대상을 찾는 루틴을 시작한다.

```
void __fastcall main_main()
{
  _QWORD *Drives; // rax
  __int64 Drive_Count; // rbx
  retval_454760 v2; // kr00_16
  __int64 v3; // [rsp+0h] [rbp-10h]
  _QWORD *v4; // [rsp+8h] [rbp-8h]

  Drives = main_getDrives();
  while ( Drive_Count > 0 )
  {
    v3 = Drive_Count;
    v4 = Drives;
    v2 = runtime_concatstring2(0, *Drives, Drives[1], ":\\", 2);
    Yurei_filewalker_EncryptDirectory(v2._r0, v2._r1);
    Drives = v4 + 2;
    Drive_Count = v3 - 1;
  }
  main_setWallpaper(Drives);
}
```

[그림 2] 현재 실행 환경의 드라이브 정보를 얻어오는 루틴

암호화 주요 파일을 잘못 암호화하여 시스템이 파괴되는 것을 방지하기 위해 암호화에서 제외되는 디렉터리, 확장자, 파일이 아래와 같이 명시되어 있다. 암호화 제외 대상 확장자와 파일의 경우 “.Yurei”, “_README_Yurei.txt” 처럼 Yurei 랜섬웨어에서 사용하는 암호화 감염 확장자를 암호화 제외 대상으로 명시하여 이미 암호화된 파일을 재감염 시키는 것을 방지하고 피해자가 랜섬노트를 확인하여 협상을 진행할 수 있도록 랜섬노트명 또한 암호화 제외 대상으로 명시하였다.

암호화 제외 대상 디렉토리
windows, system32, programdata, program files, program files (x86), public, system volume information, \system volume information, efi, boot, perflogs, microsoft, intel, appdata, .dotnet, .gradle, .nuget, .vscode, msys64

[표 1] 암호화 제외 대상 디렉토리 (19개)

암호화 제외 대상 파일 확장자
.sys, .exe, .dll, .com, .scr, .bat, .vbs, .ps1, .lnk, .inf, .reg, .msi, .ini, **.Yurei**

[표 2] 암호화 제외 대상 파일 확장자 (14개)

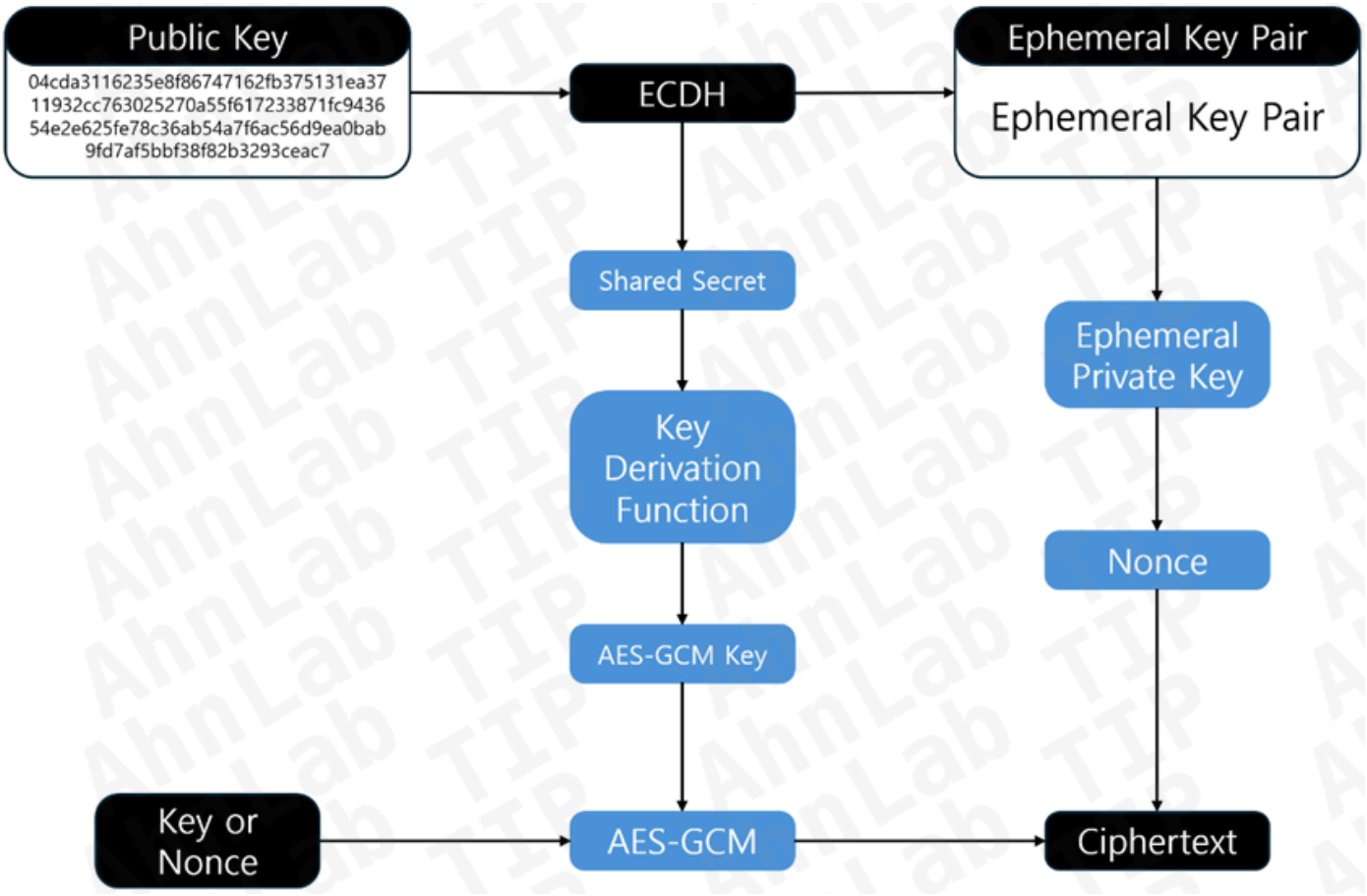
암호화 제외 대상 파일
boot, bootmgr, bcd, desktop, config, autoexec, **_README_Yurei.txt**

[표 3] 암호화 제외 대상 파일 (7개)

파일 암호화

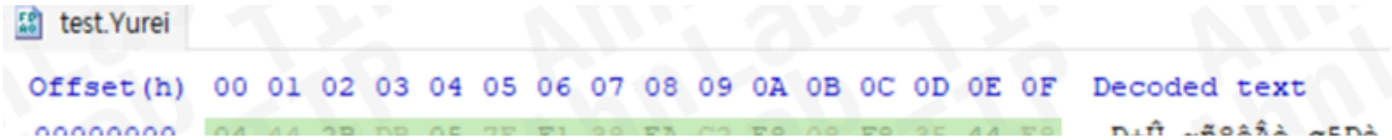
암호화 대상 파일이 최종적으로 결정되면 파일 암호화 루틴이 실행된다. 이때 Yurei 랜섬웨어는 파일 암호화에 사용할 ChaCha20-Poly1305 알고리즘의 32 Byte Key와 24 Byte Nonce를 생성한다. 생성된 Key와 Nonce는 secp256k1-ECIES 방식으로 암호화되어, 암호화된 파일 내부에 함께 저장된다.

Yurei 랜섬웨어에서 사용하는 secp256k1-ECIES 방식은 [그림 3]과 같이 랜섬웨어 내부의 Public Key와 생성된 임시 Private Key를 이용해 ECDH(Elliptic Curve Diffie-Hellman) 알고리즘으로 공유 비밀(Shared Secret)을 생성한다. 이 공유 비밀은 키 유도 함수(Key Derivation Function)를 통해 암호화에 사용할 키로 변환되며, 최종적으로 AES-GCM 알고리즘의 키로 활용된다. 이 과정에서 랜덤하게 생성된 임시 Nonce 값도 함께 사용되어 암호화 결과를 매번 다르게 만든다. 이러한 암호화 방식은 공격자가 암호화에 사용한 Key를 ECDH와 AES-GCM 방식으로 보호함으로써 네트워크에서 키가 직접 노출되지 않도록 하고, 매번 다른 임시 키를 사용해 복호화 키를 공격자가 독점할 수 있게 하여 피해자가 돈을 지불하지 않고는 데이터를 복구할 수 없도록 하기 위해서이다.



[그림 3] secp256k1-ECIES 동작 방식

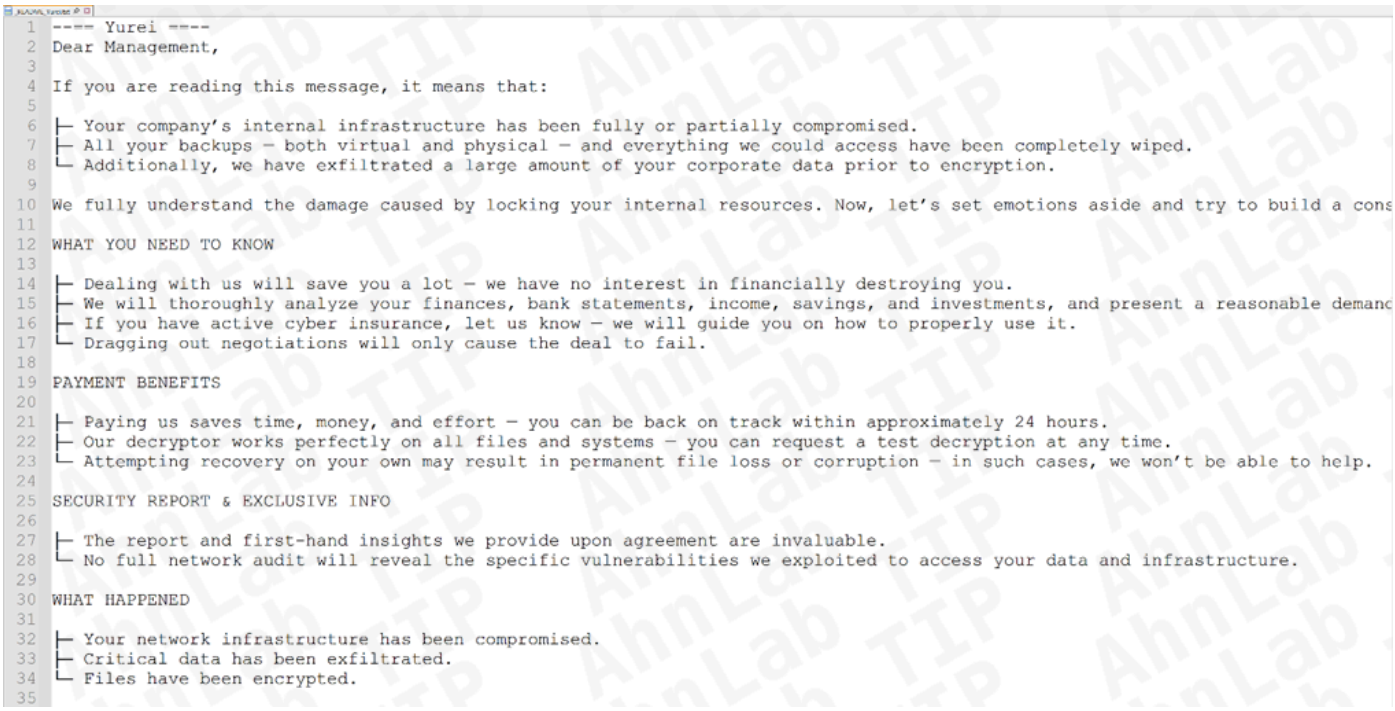
앞서 설명한 바와 같이 파일은 ChaCha20-Poly1305 알고리즘을 이용해 암호화되며, 이때 64KB 블록 단위로 처리된다. 암호화된 데이터를 기록하기 전에 [그림 4]와 같이 secp256k1-ECIES로 암호화된 32 Byte Key와 24 Byte Nonce를 “||” 마커를 기준으로 먼저 작성하고, 그 뒤에 암호화된 데이터를 순차적으로 기록한다.



[그림 4] 암호화된 파일의 구조

랜섬 노트

랜섬노트에는 기업 내부 인프라를 침해하고 접근 가능한 모든 백업을 삭제한 뒤, 대량의 데이터를 유출하고 파일을 암호화했다고 하며, 자체 복구 시도나 외부 복구 서비스 이용은 데이터 손상 및 영구 손실을 초래할 수 있다고 경고한다. 특히, 협상을 지연하거나 5일 이내에 대응하지 않을 경우 복호화 키를 삭제하고 유출된 데이터를 다크웹에 공개하거나 판매하며, 규제 기관 및 경쟁사에 통보할 수 있다고 위협한다. 또한 데이터베이스, 금융 문서, 법적 자료, 개인 정보 등 주요 데이터를 탈취했다고 강조하는 협박성 메시지가 포함되어 있다.



```
---- Yurei ----
Dear Management,

If you are reading this message, it means that:

├ Your company's internal infrastructure has been fully or partially compromised.
├ All your backups — both virtual and physical — and everything we could access have been completely wiped.
└ Additionally, we have exfiltrated a large amount of your corporate data prior to encryption.

We fully understand the damage caused by locking your internal resources. Now, let's set emotions aside and try to build a cons

WHAT YOU NEED TO KNOW

├ Dealing with us will save you a lot — we have no interest in financially destroying you.
├ We will thoroughly analyze your finances, bank statements, income, savings, and investments, and present a reasonable demanc
├ If you have active cyber insurance, let us know — we will guide you on how to properly use it.
└ Dragging out negotiations will only cause the deal to fail.

PAYMENT BENEFITS

├ Paying us saves time, money, and effort — you can be back on track within approximately 24 hours.
├ Our decryptor works perfectly on all files and systems — you can request a test decryption at any time.
└ Attempting recovery on your own may result in permanent file loss or corruption — in such cases, we won't be able to help.

SECURITY REPORT & EXCLUSIVE INFO

├ The report and first-hand insights we provide upon agreement are invaluable.
└ No full network audit will reveal the specific vulnerabilities we exploited to access your data and infrastructure.

WHAT HAPPENED

├ Your network infrastructure has been compromised.
├ Critical data has been exfiltrated.
└ Files have been encrypted.
```

[그림 5] 랜섬노트 (_README_Yurei.txt)

안랩 대응 현황

안랩 제품군의 진단명과 엔진 날짜 정보는 다음과 같다.

V3

Ransom/MDP.Event.M1785 (2017.11.23.00)

Ransom/MDP.Decoy.M1171 (2016.07.14.02)

Ransom/MDP.Event.M1875 (2018.03.10.01)

Ransomware/Win.YureiCrypt.R721068 (2025.09.08.03)

Ransomware/Win.YureiCrypt.R721188 (2025.09.08.03)

Ransomware/Win.PrinceRansom.R722378 (2025.09.10.01)

Ransomware/Win.PrinceRansom.C5753655 (2025.04.17.02)

Ransomware/Win.PrinceRansom.C5682303 (2024.10.14.02)

Ransomware/Win.PrinceRansom.C5738216 (2025.03.09.01)

Ransomware/Win.PrinceRansom.C5709845 (2024.12.24.03)

Ransomware/Win.PrinceRansom.C5685012 (2024.10.21.03)

Ransomware/Win.PrinceRansom.C5682303 (2024.10.14.02)

Ransomware/Win.PrinceRansom.C5685192 (2024.10.21.03)

EDR

Ransom/EDR.Decoy.M2470 (2022.09.29.03)
Ransom/EDR.Event.M1946 (2018.09.07.03)

MD5
1263ffe930e8ccde5bc62b043a5b6bd8

1f9700295e592ce3ea40b282e91597a2

24b4a69e3220b4e52e7c14f71e0f8dd6

32d489eef7cbbdf51dc41d07648d7d8f

331f9e123696007a9b2cc962dfb86d12

추가 IoC는 ATIP에서 제공됩니다.