KARA
Korea Anti Ransomware Alliance

2024.2Q

KARA 랜섬웨어 동향 보고서

KARA 랜섬웨어 동향 보고서

EQST Lab팀 이호석, 정민수, 이현아

랜섬웨어 트렌드

1. 2분기 Insight

OPERATION

- **Cronos : LockBit** 인프라 무력화
- **Endgame :** IcedID, SystemBC, PikaBot, SmokeLoader, Bumblebee, TrickBot **로더 및 드로퍼** 무력화

THREAT

- **국내 위협 : RansomHub**, SpaceBears, DarkVault, Underground, **IntelBroker**, 8Base
- **Top5 그룹 : LockBit**, Play, RansomHub, Inc, Medusa

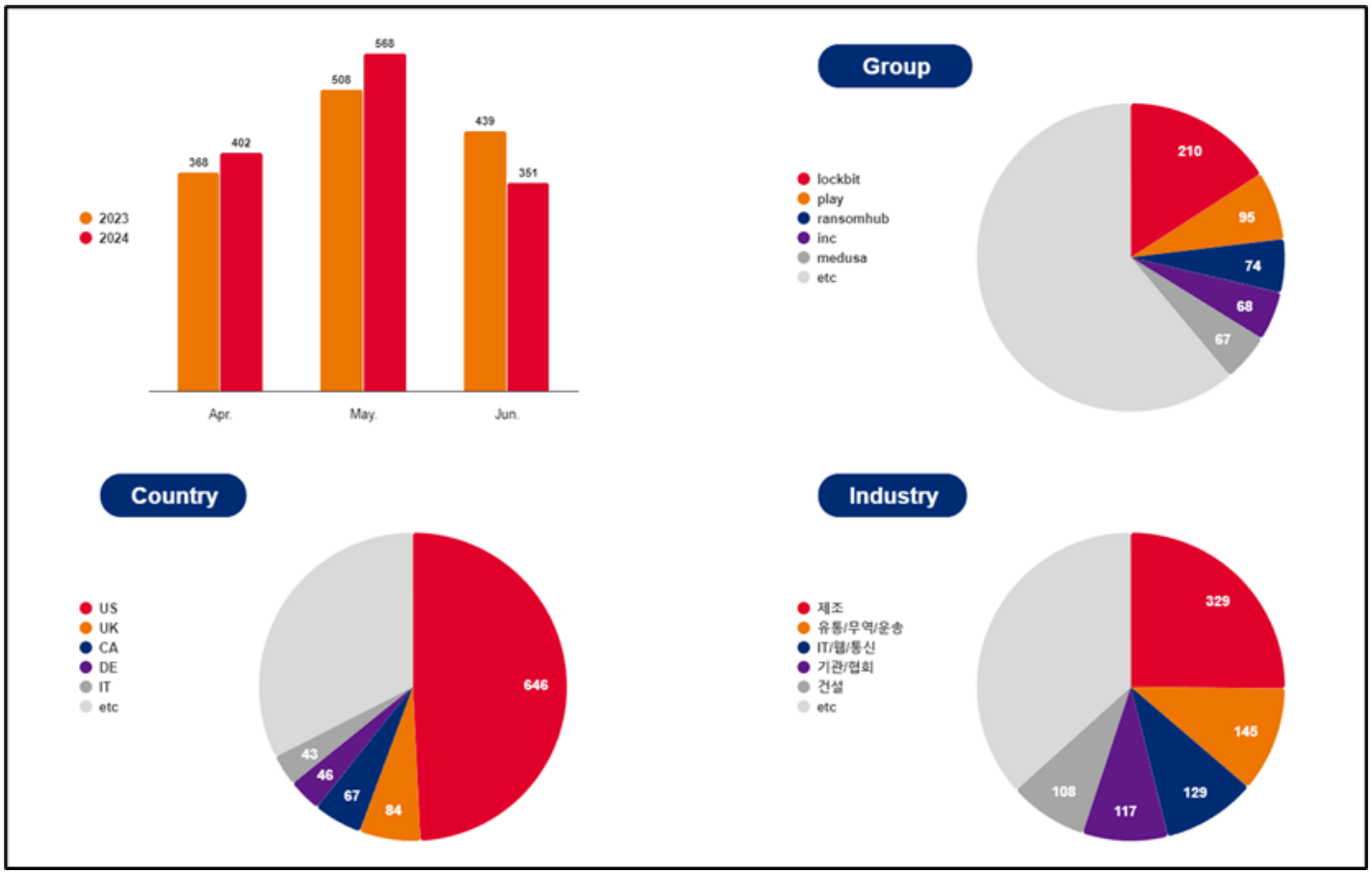
EXPLOIT

- **0-day :** CVE-2024-26169
- **1-day :** CVE-2020-1472, CVE-2024-4577, CVE-2023-27532

TARGET

- **Veeam, Windows, PHP** 취약점을 통한 초기 침투 및 **ESXi** 플랫폼 공격 증가
- 전체 공격 중 **제조업** 25%, **미국** 49%

2. 2분기 랜섬웨어 활동 통계



[랜섬웨어 그룹 활동]

2024년 2분기 랜섬웨어 피해 사례 수는 1,321건으로 작년 동기 대비 약 3% 증가한 수치를 보이고 있으며, 이번 1분기 대비 18% 증가한 수치를 보이고 있다. LockBit 그룹은 국제 수사기관의 공조로 잠시 위축되는듯 했으나 가장 많은 피해자를 게시했으며, 제조업 및 미국을 향한 공격이 가장 많이 확인됐다. 마찬가지로 Play, RansomHub, Inc, Medusa 그룹 또한 보안이 취약하고 운영 중단으로 인한 금전적인 피해가 많이 발생할 수 있는 제조업을 대상으로 공격이 가장 많이 발생했다. 전체적으로 미국과 제조업에 대한 공격이 가장 많은 수치를 보이고 있지만 Inc, Medusa 그룹은 제조업과 더불어 의료 및 기관을 향한 공격이 가장 많이 발견되기도 했다.

Cronos 작전[1], Endgame 작전[2]과 같은 국제 공조를 통한 공격자 체포 및 인프라 무력화 작전과 더불어 여러 사이버 범죄자들의 체포 소식이 들려오고 있으나, 생성형 AI 악용, BitLocker[3] 악용, 취약점 악용 등의 다양한 전략을 통해 피해 사례가 꾸준히 증가하고 있는 모양새다. 국제적으로 수사 기관들이 협력하여 주요 공격자들을 색출해 내고 있지만 랜섬웨어 그룹들은 전략의 다변화와 타깃 플랫폼의 확장을 통해 교묘하고 더 큰 위협으로 다가오고 있다.

---

[1] Cronos 작전 : LockBit의 공격 서버, 다크웹 유출 사이트 등 범죄 인프라를 파괴하기 위한 국제 수사기관의 공조 작전

[2] Endgame 작전 : 랜섬웨어를 배포하는데 사용되는 로더나 드로퍼 악성코드 인프라를 파괴하기 위한 국제 수사기관의 공조 작전

[3] BitLocker : Windows 환경에서 데이터를 보안을 유지하기 위해 디스크를 암호화 하는 기능

LockBit 그룹은 국제 공조를 통한 Cronos 작전 이후 새로운 인프라를 통해 활동을 재개했지만, 핵심 인물인 'LockBitSupp'의 신상이 공개되고 기소됐다. 또한 Cronos 작전 발표 직후 공개한 피해 기업 53건은 절반 정도가 다시 게시된 기업들이었고, 미국의 중앙은행을 공격했다는 허위성 주장과 테스트 게시글 노출, 호스팅 되는 인프라가 드러나고 유출 사이트 접속이 되지 않는 등 가장 위협이 되고 있는 그룹으로 보기 힘든 모습을 보였다. 불안정한 운영으로 인해 리브랜딩 혹은 활동을 종료하기 위한 분위기가 보였지만, 이를 의식한 LockBit은 유출 데이터를 꾸준히 게시하는 모습을 통해 그룹의 건재함을 과시하며 활동을 이어가고 있다.

Play 랜섬웨어 그룹은 5월에 ESXi 버전을 출시하며 공격 대상 플랫폼을 추가했다. ESXi 환경은 일반적으로 기업에서 비용 절감을 위해 하나의 물리적 서버로 여러 가상 머신을 실행해 어플리케이션과 백업 솔루션을 호스팅 하는데 주로 사용한다. 만약 ESXi 환경이 암호화될 경우 서비스 운영에 크게 차질을 빚게 되고, 백업 솔루션을 호스팅 중이었다면 백업한 리소스를 활용할 수 없는 경우가 발생할 수 있어 많은 랜섬웨어 그룹이 공격 타깃으로 삼고 있다. Play의 ESXi 변종은 ESXi 환경에서 실행될 경우에만 암호화를 수행하며 VM 디스크, 구성 파일, 메타 데이터 파일 등 중요한 파일들을 모두 암호화한다.

RansomHub는 올해 2월에 발견된 그룹으로 Knight 랜섬웨어의 리브랜딩이다. RansomHub는 BlackCat(Alphv)이 Exit Scam[4]으로 활동을 종료하고 갈 곳을 잃은 계열사들이 합류한 뒤로 더욱 많은 공격 사례가 확인되고 있으며 Scattered Spider 해킹 그룹이 RansomHub 랜섬웨어를 공격에 사용하는 등 파급력 있는 랜섬웨어 그룹으로 자리 잡았다. 또한 그 영향이 국내까지 확산되어 한 건설 회사가 타격을 입은 사례도 확인됐다. RansomHub는 Go 언어[5]로 개발된 Linux, Windows 버전과 C++로 개발한 ESXi 변종이 존재하며, 그중 ESXi 버전은 PID[6]가 기록된 /tmp/app.pid 파일을 사용해 중복 실행을 확인한다. 만약 파일이 존재할 경우 먼저 실행된 랜섬웨어 프로세스를 종료하려고 시도하는데 파일의 PID 값을 "-1"로 변경하면, 랜섬웨어는 존재하지 않는 프로세스 ID (-1)로 종료를 시도해 무한 루프에 빠져 파일을 암호화 시키지 못하는 결함이 존재한다.

Inc 랜섬웨어 그룹은 v1, v2 샘플이 존재하는데, 최신 버전인 v2는 4월에 생성된 변종이다. v2가 생성된 이후인 5월에 소스코드를 판매하려는 움직임이 포착됐는데, 판매자는 해킹 포럼에서 Inc 랜섬웨어의 소스코드를 30만 달러(한화 약 4억 원)에 판매하겠다는 의사를 표하며 상세 정보를 게시했다. 보통 소스코드를 판매하는 경우 활동을 중단하거나 리브랜딩 후 새로운 활동을 시작하지만 현재까지 피해자를 꾸준히 게시하며 위협 행위를 이어가고 있다.

Medusa 그룹은 2023년 2월부터 의료 기관을 포함한 여러 기업에 대한 공격을 수행하고 몸값을 요구하는 등 꾸준한 행보를 보이고 있다. Medusa 랜섬웨어 그룹은 피해를 입은 조직과의 협상에서 50만 달러(한화 약 7억 원), 77만 달러(한화 약 11억 원), 150만 달러(한화 약 21억 원) 등 고액의 몸값을 요구하며 피해자들을 협박하고 있다.

3. 랜섬웨어 트렌드

✓ 2분기 국내 랜섬웨어 피해

2분기 국내 랜섬웨어 피해 사례 수는 10건으로, 지난 분기 대비 9건이 증가한 수치를 보이고 있다. 특히 제조 업에 가장 많은 피해 사례가 발생했으며, 가장 많은 공격을 수행한 공격자는 IntelBroker이다. IntelBroker는 유명 해킹 포럼인 BreachForums에서 활발한 활동을 이어나가고 있으며, 국내 공공 기관 두 곳의 데이터베이스와 잡화 판매 업체의 데이터베이스를 유출 시켰다. 특히 한 공공 기관의 유출 데이터베이스를 공개한 건에 대해서는 해당 기관의 관계자가 가짜 데이터를 게시한 것이라고 밝혔지만, 서버에서 직접 추출한 형태의 덤프 데이터이며 포럼에서 평판이 비교적 좋은 공격자임을 감안하면 실제로 취득한 데이터일 확률도 존재한다.

---

[4] Exit Scam : 계열사에게 지급해야할 대금을 정산하지 않은 채 잠적하는 사기 행위

[5] Go 언어 : 구글에서 개발한 프로그래밍 언어로, 컴파일 한 바이너리가 크고 복잡하여 분석이 어려움

[6] PID : 운영체제가 각 프로세스를 식별하기 위해 할당하는 고유한 숫자

IntelBroker뿐 아니라 BreachForums의 또 다른 유저가 국내의 한 스타트업 기업의 데이터 13GB 가량을 유출 했다고 주장하기도 했다. 또한 국내 한 식품 제조 업체의 2023년 7월 데이터를 탈취했다고 주장하는 유저는 연락처를 포함한 정보 유출을 주장해 2차 피해가 우려되는 상황이다.

✓ Cronos 작전에 연이은 Endgame 작전

올해 2월, 악명 높은 랜섬웨어 그룹인 LockBit의 인프라를 무력화 시키고 관련 인물들을 수사하는 Cronos 작전이 펼쳐졌다. 이후 LockBit을 완전히 무너트리지는 못했지만, 현재 과거와는 다른 모습을 보이고 있어 상당한 타격을 받은 것으로 볼 수 있다. Cronos 작전 이후 또 한 번 랜섬웨어 생태계에 큰 타격을 준 작전인 Endgame이 5월에 펼쳐졌다. Endgame은 랜섬웨어를 배포하는 로더 및 드로퍼를 무력화 시키는 작전으로 대표적으로 IcedID, SystemBC, PikaBot, SmokeLoader, Bumblebee, TrickBot이 이에 해당된다. 해당 작전을 통해 100개가 넘는 서버가 다운되고 핵심 인물들의 신원이 공개되고 체포됐다. Endgame으로 무력화된 드로퍼는 DarkSide, BlackBasta, Stop, Phobos 등의 랜섬웨어가 보안 솔루션의 탐지를 우회할 수 있게 도와주는 역할을 수행한다. 국제 수사 기관은 이러한 작전을 통해서 랜섬웨어와 직간접적으로 연관이 있는 인프라를 선제적으로 무력화 시키는 움직임을 지속적으로 보이고 있다.

✓ 랜섬웨어 그룹의 취약점 악용

2분기에도 랜섬웨어 그룹들은 다양한 취약점을 악용해 초기 침투 후 랜섬웨어 공격을 수행했다. 특히 급격한 성장세를 보이고 있는 RansomHub 그룹은 오래된 취약점인 CVE-2020-1472 취약점을 악용한 공격 사례가 확인됐다. 해당 취약점은 ZeroLogon이라고도 불리는 취약점인데, Windows Server에서 도메인 사용자 인증을 담당하는 Netlogon 서비스에서 도메인 컨트롤러와의 보안 채널 연결을 무력화시켜 관리자 권한을 획득할 수 있다. RansomHub는 이를 악용해 시스템의 관리자 권한 획득 후 랜섬웨어 공격을 수행했다.

한편 PHP 취약점 CVE-2024-4577을 악용한 TellYouThePass 랜섬웨어 공격은 공개된 PoC를 악용해 PHP 서버에 원격으로 악성 HTA 파일을 실행시킨 뒤 랜섬웨어를 메모리에 로드했다. 피해자에게 6,700 달러(한화 약 930만 원)를 요구하기도 했는데, 해당 공격은 PoC가 공개된 지 하루 만에 발생해 공개된 익스플로잇 코드가 실제 공격에 빠르게 악용될 수 있음을 시사한다.

꾸준한 활동을 보이고 있는 Akira 그룹과 Estate 랜섬웨어 역시 발견된 지 1년 이상 지난 취약점인 CVE-2023-27532를 악용한 것으로 확인됐다. CVE-2023-27532는 Veeam Backup & Replication[7]의 취약점으로 해당 취약점을 통해 침투 후 계정을 생성해 보안 솔루션을 무력화했으며 이후 랜섬웨어를 실행했다.

오래된 취약점뿐만 아니라 공격자들은 제로데이 취약점을 발견해 공격에 사용한 정황도 확인됐다. BlackBasta 그룹은 Windows Error Reporting Service[8]의 권한 상승 취약점(CVE-2024-26169)을 악용해 초기 침투를 시도했으며, 공격이 이루어진 시기는 취약점 패치가 공개되기 전으로 확인된다. 이처럼 랜섬웨어 그룹들은 다양한 취약점을 악용해 초기 침투를 수행하고 있어 이를 예방하기 위해 최신 버전의 시스템 환경을 유지하는 것이 강조된다.

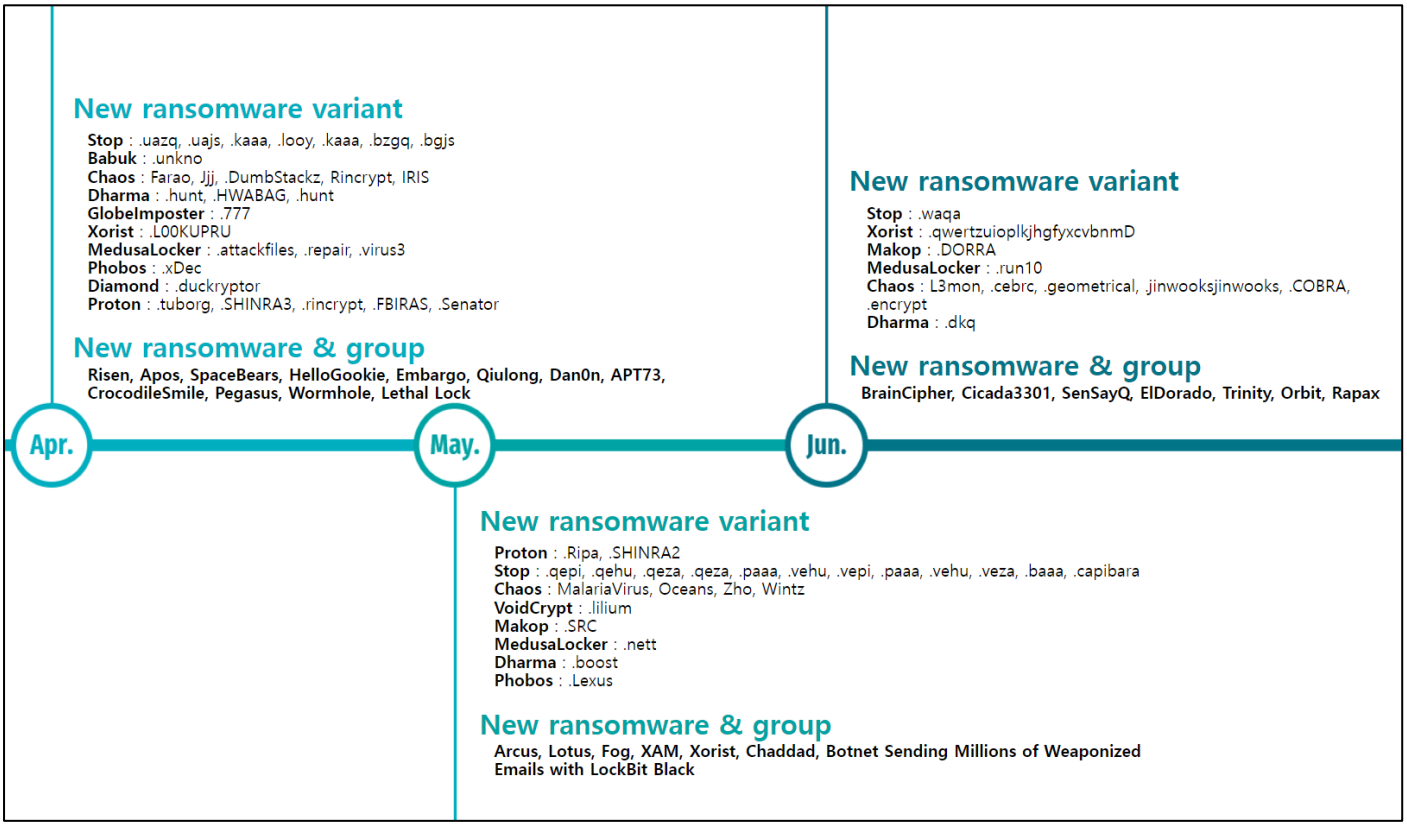
[7] Veeam Backup & Replication : 데이터 백업 및 복구 솔루션

[8] Windows Error Reporting Service : Windows 시스템의 오류 보고를 처리하는 서비스

CVE	악용 공격자	설명	영향 버전
CVE-2020-1472	RansomHub	Netlogon 서비스에서 도메인 컨트롤러와 보안 채널을 무력화시켜 권한 상승	Windows Server 2008~2019
CVE-2023-27532	Akira, Estate	인증되지 않은 사용자가 데이터 베이스에 저장된 호스트 자격 증명을 조회 가능	Veeam Backup & Replication V12, V11a
CVE-2024-4577	TellYouThePass	Windows의 Apache와 PHP-CGI 사용시 일본어 및 중국어 코드 페이지 설정에 의해 명령 줄 인자가 잘못 해석되어 임의 PHP 코드 실행 가능	PHP 8.1.*(<8.1.29) PHP 8.2.*(<8.2.20) PHP 8.3.*(<8.3.8)
CVE-2024-26169	BlackBasta	Windows Error Reporting Service에서 발생하는 권한 상승 취약점	Windows 10 1507, 1607, 1809, 21H2, 22H2 Windows 11 21H2, 22H2

[2분기에 랜섬웨어 그룹이 악용한 취약점 목록]

4. 신규 랜섬웨어 및 그룹 활동



[신규/변종 랜섬웨어]

2 분기에도 16 개의 다양한 신규 랜섬웨어 그룹이 발견됐다. 4 월에 발견된 신규 랜섬웨어 그룹 Risen 은 현재 DLS[9]가 접속 불가인 상태이다. 이들은 해킹 포럼에서 자신들의 랜섬웨어를 소개하는 글을 게시하며 홍보하기도 했다. Apos 는 노션을 사용하여 피해자 4 건 게시 후 삭제한 뒤 현재는 활동하는 모습이 보이지 않는 상태이다. Qiulong 그룹은 발견 이후 현재까지 활동하고 있는 그룹인데, 게시된 피해 기업은 총 8 곳으로 7 군데가 브라질 기업으로 주로 의료 산업을 대상으로 공격을 수행했다. 같은 시기 발견된 Dan0n 그룹은 총 16 개의 기업에 대한 글을 게시했고, 그중 15 곳이 미국이고 나머지 한 곳은 아일랜드에 해당된다.

5 월에 발견된 Arcus 그룹은 Arcus Media 라는 DLS 를 운영하고 있다. 6 월까지 총 25 개의 기업에 대한 공격 글을 게시했으며, 많은 수의 피해 기업이 브라질에 위치하고 있다. 6 월에 발견된 Cicada3301 그룹은 고도의 지능을 갖춘 사람을 모집 중이라고 주장하는 인터넷 집단과 같은 이름을 사용하고 있으며 DLS 에 총 4 개의 기업에 대한 피해 사례를 게시했다. SensayQ 그룹은 유출된 LockBit Black 빌더[10]를 악용하여 만들어진 랜섬웨어를 공격에 사용하고 있는 것으로 확인됐다. Trinity 그룹은 DLS 에 총 3 개의 피해 사례를 게시했으며, 랜섬웨어는 2023Lock 과 동일한 랜섬노트를 사용하는 것으로 확인된다. 아래는 2 분기에 발견된 주요 랜섬웨어 그룹에 대한 설명이다.

- **SpaceBears**

  SpaceBears는 러시아에 기반을 둔 랜섬웨어 그룹으로, 국내의 한 제조 기업을 포함하여 6월까지 20개의 중소규모 기업에 대해 공격 후 유출 데이터를 게시했다. 클리어 웹[11]에서 호스팅 되는 Gofile[12]을 통해 데이터를 공개해 다운로드할 수 있는 시간이 제한적이라는 특징이 있다. SpaceBears 측은 만약 피해자가 몸값을 지불한다면 그 대가로 데이터를 삭제하고 향후 유사한 공격에 피해를 입지 않는 방법을 컨설팅 해주겠다고 주장하고 있다.

- **HelloGookie**

  HelloGookie는 HelloKitty의 리브랜딩 버전이다. 2020년 11월에 활동을 개시한 HelloKitty는 외국의 한 게임회사를 공격해 랜섬웨어 공격을 수행하고 게임의 소스코드와 데이터를 탈취해 다크웹에 판매했다고 밝혔다. 또한 ESXi를 타깃으로 한 변종을 출시하며 공격 대상을 넓혀나갔다. 이후 2023년 10월 무렵에 Gookee 및 kapuchino라는 닉네임으로 해킹 포럼에서 활동하던 HelloKitty 개발자는 초기 버전의 소스코드와 빌더를 공개하며 운영을 종료한 뒤 HelloGookie로 재등장 했으나, 아직 DLS에 게시된 피해 기업은 없는 것으로 확인된다.

- **Embargo**

  Embargo 랜섬웨어 그룹은 4월에 활동을 시작했으며, 6월까지 DLS에 게시된 기업은 8개이다. 사용하는 랜섬웨어는 Rust 언어[13]로 제작됐으며, ChaCha20으로 파일을 암호화하고 Curve25519로 해당 키를 보호한다는 특징이 있다. 평균적으로 피해 기업에 요구하는 몸값은 약 100만 달러(한화 약 14억 원)로 상당히 높은 금액을 요구하고 있다.

---

[9] DLS(Dedicated/Data Leak Site) : 탈취한 데이터를 게시하여 피해자를 협박하는 데 사용하는 다크웹 유출 사이트

[10] 빌더 : 사용자 정의 랜섬웨어를 제작할 수 있도록 도와주는 도구

[11] 클리어 웹 : 검색을 통해 접근할 수 있는 일반적인 웹 사이트

[12] Gofile : 파일을 공유하는 클라우드 기반 서비스

[13] Rust 언어 : 메모리 관리에 중점을 둔 프로그래밍 언어로, 컴파일된 바이너리는 구조가 복잡해 분석이 어려움

- **APT73**

  외국의 한 보안 벤더에서 특정 국가나 조직의 이익을 위해 해킹 활동을 하는 사이버 범죄 단체에 대해 APT라고 명명하고 있는데, APT73이라는 랜섬웨어 그룹은 특이하게 APT를 포함한 이름으로 활동하고 있으며, eraleignews라는 클리어 웹을 개설한 이력으로 Eraleig로 부르기도 한다. 해당 그룹은 주로 영국을 대상으로 공격했으며, IT 산업 군에 가장 많은 피해를 입혔다.

- **Fog**

  Fog는 5월에 발견된 랜섬웨어 그룹으로, HC-256 알고리즘을 사용해 파일을 암호화하고 RSA로 해당 키를 보호한다는 특징이 있다. Fog 그룹은 주로 탈취된 VPN[14] 자격 증명을 통해 초기 침투를 수행하며, 교육 및 레크리에이션 산업에 대해서 공격을 수행했다. 활동 초반에는 단일 협박 방식을 사용했으나, 현재는 DLS에 피해 기업에 대한 데이터를 게시하며 이중 협박 방식을 통해 피해자에게 몸값을 요구하고 있다.

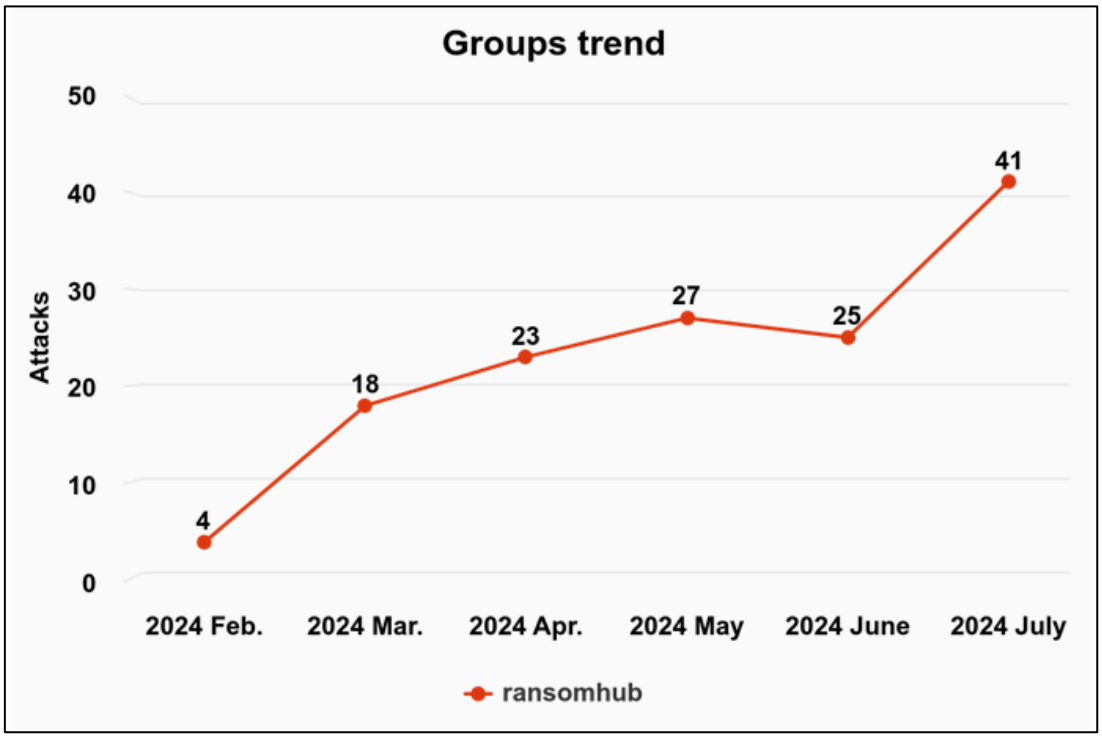
- **Eldorado**

  Eldorado 랜섬웨어 그룹은 6월에 발견된 그룹으로, DLS를 개설 후 15개의 피해 기업을 공개했다. 이들이 사용하는 Embargo 랜섬웨어는 Go 언어로 제작됐으며 ChaCha20으로 파일을 암호화하고 RSA로 해당 키를 보호하는 특징이 있다. 또한 랜섬웨어에 감염되었을 때 생성되는 랜섬노트 내용이 LostTrust의 랜섬노트 형식과 동일해 연관성이 의심된다.

[14] VPN(Virtual Private Network) : 개인 정보를 암호화 하고 IP 주소를 숨겨 안전하게 데이터 통신을 할 수 있게 해주는 네트워크 기술

RansomHub 그룹 상세 분석

1. RansomHub 개요



[RansomHub 그룹의 공격 건수]

RansomHub 그룹은 Knight 랜섬웨어의 리브랜딩으로, Go 언어로 제작됐으며 Gobfuscate[15]를 통해 난독화되어 있다는 특징이 있다. 사용된 코드 및 랜섬노트, 실행 시 전달되는 인자가 상당부분 유사해 리브랜딩으로 보고있으며, Knight 가 활동을 종료한 시기와 RansomHub 가 활동을 개시한 시기가 비슷해 리브랜딩의 근거를 뒷받침 해주고 있다. RansomHub 는 Zerologon 취약점(CVE-2020-1472)[16]을 통해 초기 침투를 하기도 하며 Atera, Splashtop 와 같은 RMM 도구[17]를 통해 접근하기도 했으며, NetScan[18]을 통해 네트워크 스캔 작업을 수행하여 확산을 시도하기도 한다. 뿐만 아니라 iisreset.exe 혹은 iisrstas.exe 와 같은 도구를 활용해 백업으로 사용되는 IIS 서비스[19]를 중단시켜 복구를 하기 어렵게 만들기도 했다. RansomHub 가 이렇게 활발한 활동을 할 수 있게 된 계기는 이전 BlackCat(Alphv)의 핵심 계열사인 Noberus 를 영입한데다, Scattered Spider[20]와 협력하고 있기 때문이라고 할 수 있다.

---

[15] Gobfuscate : Go 언어로 작성된 코드를 난독화하여 분석이 어렵게 만드는 도구

[16] Zerologon 취약점(CVE-2020-1472) : Netlogon Remote Protocol을 이용해 도메인 컨트롤러에 취약한 보안 채널 연결을 설정하고 도메인 관리자 접근 권한을 획득하는 권한 상승 취약점

[17] RMM 도구 : 원격으로 시스템을 관리할 수 있게 하는 도구

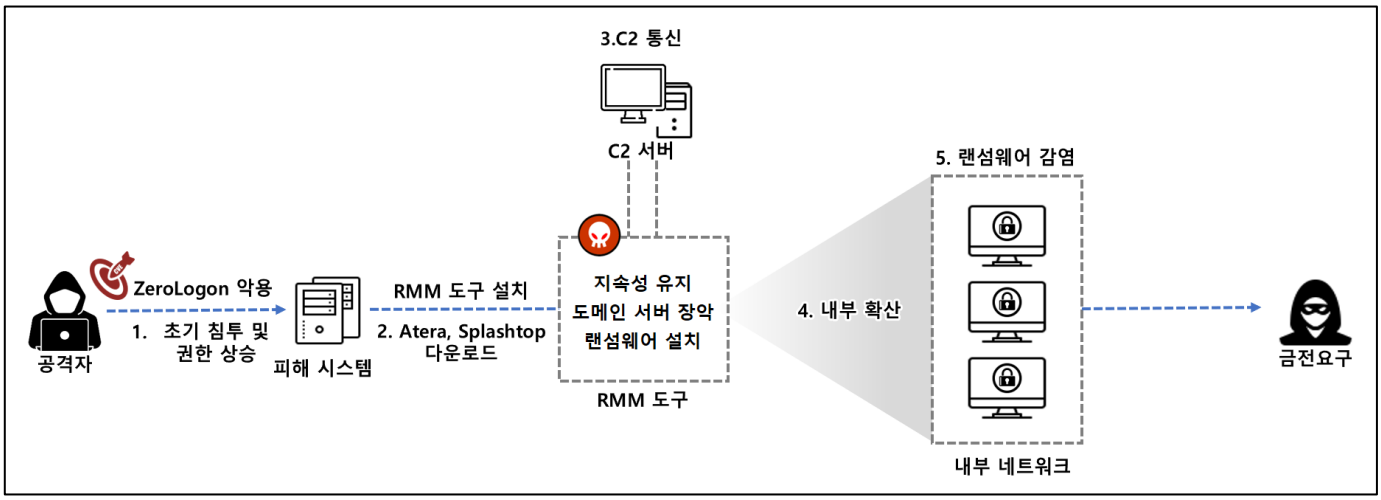
[18] NetScan : 네트워크에 존재하는 호스트를 검색하고 특정 포트의 상태를 스캐닝하는 도구

[19] IIS 서비스 : 웹 서버 소프트웨어로 웹 사이트 호스팅 및 관리를 위해 사용

[20] Scattered Spider : RansomHub, Qilin 랜섬웨어를 통해 공격을 수행하는 사이버 범죄 그룹

BlackCat(Alphv)이 Exit Scam 을 통해 종적을 감춘 탓에 대금을 지불 받지 못한 계열사의 사례가 존재했다. 이를 지켜본 다른 계열사들이 같은 문제가 반복될까 노심초사하고 있는 시기에 RansomHub 는 피해자에게 갈취한 대금을 그룹 관리자가 먼저 받아서 정산해 주는 기존의 방식이 아닌, 계열사에게 선 지급 후 크레딧을 가져가는 형식으로 홍보하고 있다. 이는 계열사에게 유리한 형태의 운영 방식으로 RansomHub 가 많은 계열사를 유치해 몸집을 키워 나가는데 일조한 것으로 추측된다.

2. RansomHub 공격 시나리오



[RansomHub 공격 시나리오]

RansomHub 랜섬웨어 공격자는 ZeroLogon 취약점을 통해 초기 침투 후 권한 상승을 통해 RMM 도구를 설치하고 랜섬웨어를 감염시켰다. 해당 취약점은 NetLogon 원격 프로토콜(NS-NRPC)에 존재하며, 이는 Windows 서버가 도메인[21] 내에서 사용자와 서비스를 인증하는 데 사용된다. 이때 ZeroLogon 취약점을 악용하면 인증 없이 도메인 컨트롤러[22]를 포함한 모든 컴퓨터에 대한 권한을 얻을 수 있다.

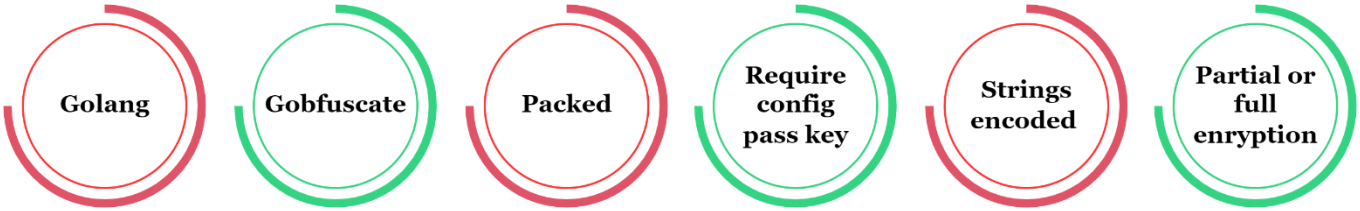
이후 지속적으로 시스템에 접근하기 위해서 RMM 도구를 설치하고, 내부 전파를 위해 네트워크 정보 수집 도구인 NetScan 을 설치하기도 했다. RMM 도구인 Atera 와 Splashtop 은 일반적으로 널리 사용되는 원격 접근 및 관리 도구다. 정상적인 프로그램으로 인식돼 보안 솔루션에 탐지되지 않는 특징이 있어 피해 시스템에 지속적으로 접근하기 위해 설치했다. NetScan 도구는 네트워크 스캐닝 도구로, 연결된 네트워크를 탐지하는 기능을 수행한다. 해당 도구를 통해 공격자는 서버, 데이터베이스, 기타 주요 인프라 등을 식별했고, 연결된 내부 네트워크에 랜섬웨어를 모두 감염시켰다. 이후 주요 데이터를 탈취하고 랜섬웨어를 전체 시스템에 감염시킨 공격자는 이를 빌미로 금전을 요구했다.

[21] 도메인 : 네트워크에 연결된 컴퓨터, 사용자, 자원을 하나의 그룹으로 관리하는 환경

[22] 도메인 컨트롤러 : 도메인 내에서 사용자 인증과 권한 관리를 담당하는 서버

3. RansomHub 심층 분석

✓ 특징



- RansomHub 랜섬웨어는 Go 언어로 제작됐으며, Gobfuscate를 통한 난독화로 인해 함수 이름과 변수, 타입 상수 등 심볼 정보가 숨겨져 있다.
- 또한, 실행에 필요한 설정값이 암호화되어 있으며 복호화에 필요한 키값을 실행 시 -pass 인자를 통해 전달해 pass 키가 없는 경우 정상적으로 실행이 되지 않는다.
- 암호화된 설정값뿐만 아니라 실행에 필요한 문자열이 각각 고유한 키로 인코딩[23]되어 있어 실행 중 필요할 때마다 디코딩[24] 후 사용한다.
- 빠른 암호화를 위해 파일 크기에 따라 다른 암호화 방식을 사용하며 2MB 이상 파일의 경우 부분 암호화를 사용한다.

✓ 랜섬웨어 그룹 유사성

RansomHub 랜섬웨어는 BlackCat(Alphv), Knight(CyClops의 리브랜딩 버전) 랜섬웨어와 유사성을 확인할 수 있다. BlackCat 랜섬웨어에서 사용한 랜섬노트의 일부 문구가 동일하며, JSON 형태의 설정값이 유사하다. 하지만, 이는 BlackCat 랜섬웨어의 일부 특성을 차용한 것으로 보이며 오히려 Knight 랜섬웨어와 매우 유사함을 보인다. 랜섬노트의 비슷한 문구 사용과 실행 시 전달되는 옵션 및 코드 유사도가 아주 높아 Knight 랜섬웨어의 업데이트된 버전으로 볼 수 있다. 또한, Knight 랜섬웨어는 다크웹 데이터 유출 사이트에 2024년 2월 8일 공개한 피해자를 마지막으로 게시했지만 RansomHub 다크웹 데이터 유출 사이트가 2024년 2월 5일 발견되어 이미 새로운 버전을 준비한 것으로 보이며, 최초 피해자 게시일이 2024년 2월 10일인 것도 시기상 겹치는 것을 확인할 수 있다. 이러한 증거를 종합적으로 검토해 보면 RansomHub 랜섬웨어는 Knight 랜섬웨어의 리브랜딩 버전으로 볼 수 있다.

[23] 인코딩 : 데이터를 이해하기 어려운 형태로 변환하여 분석을 어렵게 함

[24] 디코딩 : 인코딩을 해제하여 원본 데이터로 복원하는 과정

- **RansomHub ≒ BlackCat(Alphv)**

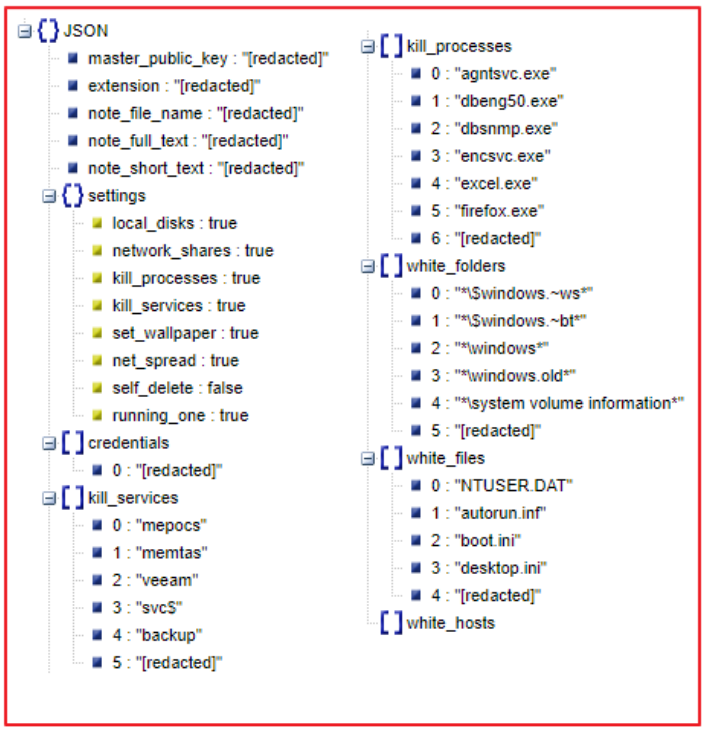
BlackCat(Alphv) 그룹에서 사용한 랜섬노트 중 일부 문구가 RansomHub 랜섬노트에 그대로 사용된 흔적이 발견됐다. '>>> WARNING', '>> CAUTION' 문구만 다르고 경고를 알리는 문장이 똑같은 것을 확인할 수 있다.

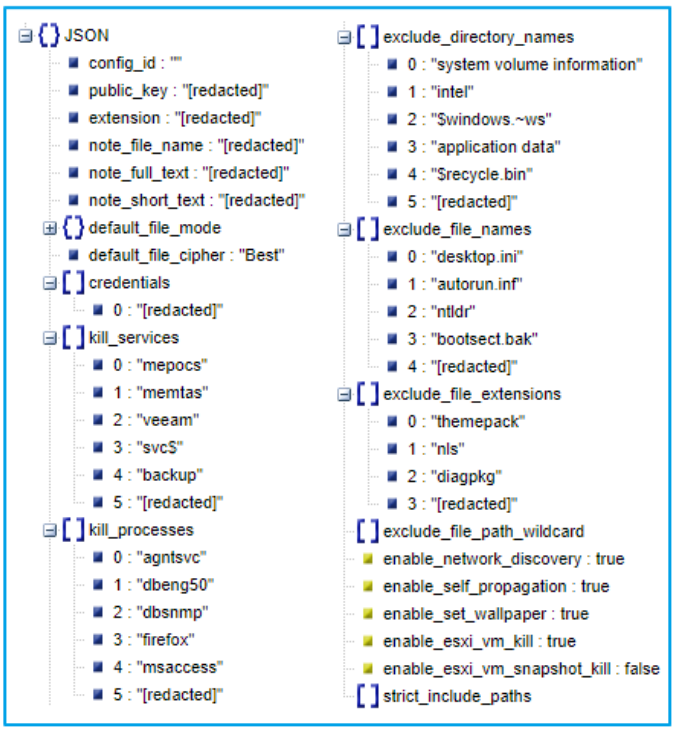
```
>>> WARNING

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
```

```
>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
```

[RansomHub(상), BlackCat(하) 랜섬노트 일부]

BlackCat(Alphv) 랜섬웨어와 또 다른 유사점은 랜섬웨어 실행에 필요한 설정값을 암호화해 내부 바이너리로 포함하고 있으며, 실행 시 전달되는 키를 통해 동적으로 복호화 후 사용한다. BlackCat(Alphv) 랜섬웨어는 설정값 복호화를 위해 실행 시 '-access-token' 인자가 필요하며, RansomHub는 실행 시 전달되는 '-pass' 값을 통해 암호화된 설정값을 복호화 후 사용한다. 복호화 된 설정값은 JSON 형태이며 일부 항목과 데이터들을 유사하게 사용하고 있음을 확인할 수 있다.





[RansomHub(좌), BlackCat(우) config JSON 일부]

- **RansomHub ≒ Knight**

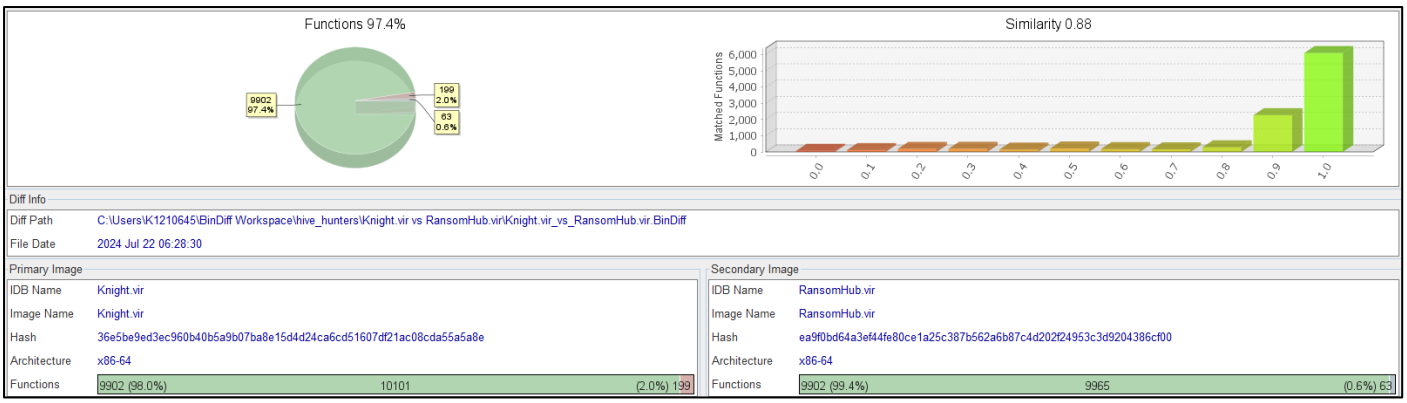
RansomHub 랜섬웨어는 네트워크 비활성화, 특정 호스트 혹은 경로만 암호화, 안전 모드에서 동작 등 다양한 옵션을 제공하고 있다. 여기서 주목할 점은 과거 Knight 랜섬웨어의 실행 옵션과 상당히 유사하다는 것이다. 단순히 -sleep 옵션이 추가된 정도의 차이만 존재한다.

```
C:₩Sample>RansomHub.exe -help
USAGE: RansomHub.exe [OPTIONS]
OPTIONS:
  -disable-net
        disable network before running
  -host value
        only process smb hosts inside defined host. -host 10.10.10.10 -host 10.10.10.11
  -only-local
        only encrypt local disks
  -pass string
        Pass
  -path value
        only process files inside defined path. -path C:// -path D:// -path //10.10.10.10/d/
  -safeboot
        reboot in Safe Mode before running
  -safeboot-instance
        run as Safe Mode instance
  -sleep int
        sleep for a period of time to run (minute)
  -verbose
        log to console
```

추가된 옵션

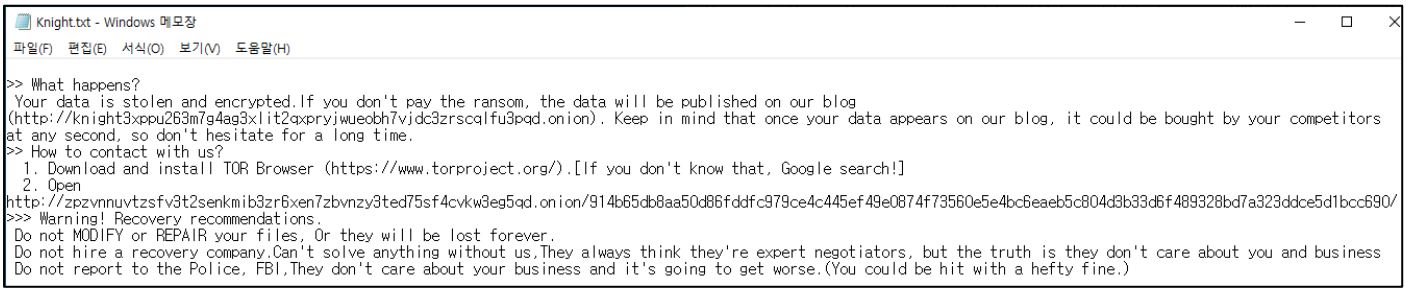
[RansomHub 실행 옵션 설명]

Knight, RansomHub 샘플 모두 Go 언어로 제작됐으며, Gobfuscate 난독화 기법을 사용했다. 두 샘플을 비교해 보면 함수 매칭 97.4%, 1이면 동일한 것으로 간주하는 유사도 수치는 0.88로 상당수의 코드가 중복되는 것을 확인할 수 있다.



[RansomHub와 Knight 랜섬웨어 유사도 비교]

Knight 랜섬웨어의 랜섬노트와 RansomHub에서 사용하는 랜섬노트 사이에도 유사한 문구가 사용됐으며, 이는 기존 노트를 일부 수정 후 사용했거나, 단순히 차용해 사용했을 수도 있는 부분을 확인할 수 있다.

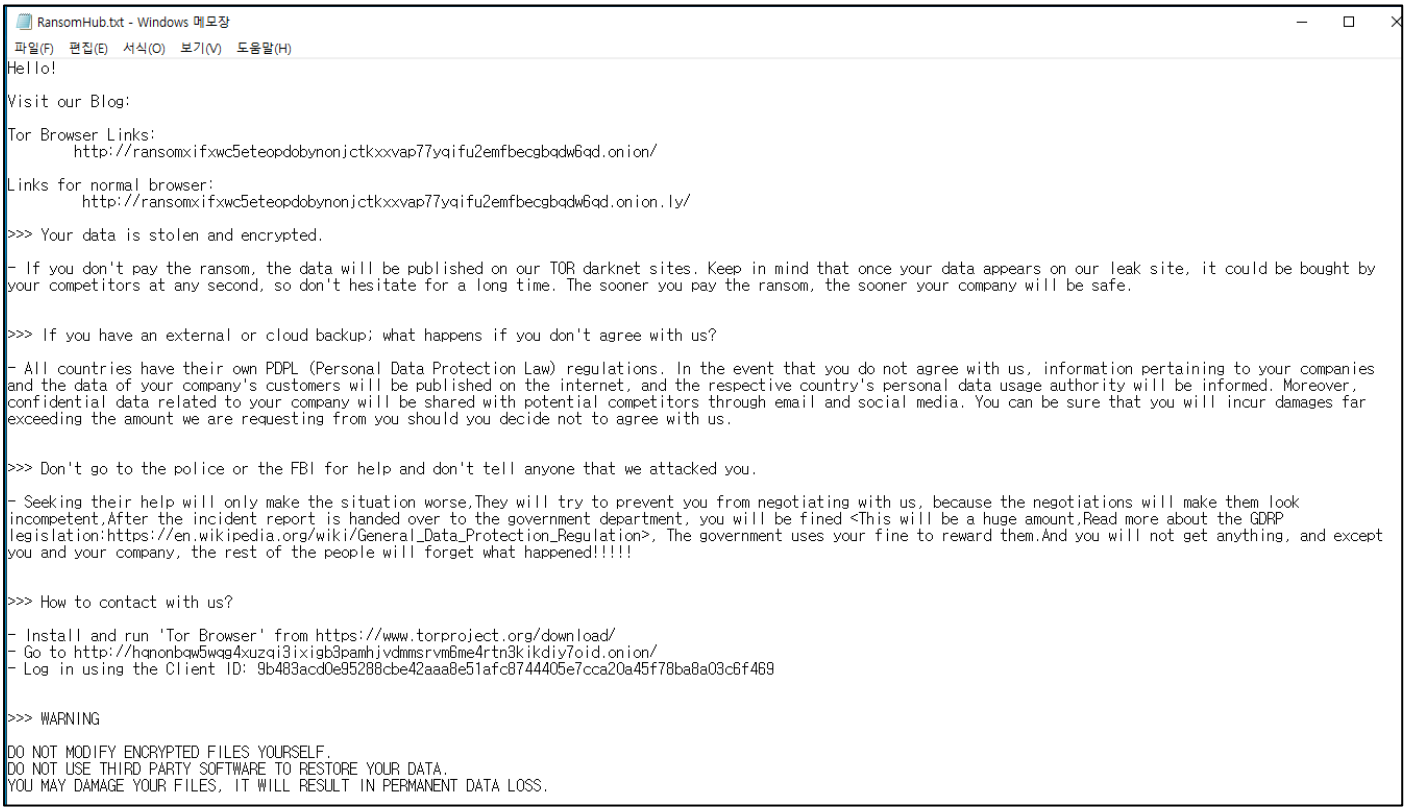


Knight.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
>> What happens?
 Your data is stolen and encrypted.If you don't pay the ransom, the data will be published on our blog
(http://knight3xppu263m7g4ag3xlit2qxpryjwueobh7vjdc3zrscqlfu3pqd.onion). Keep in mind that once your data appears on our blog, it could be bought by your competitors
at any second, so don't hesitate for a long time.
>> How to contact with us?
  1. Download and install TOR Browser (https://www.torproject.org/).[If you don't know that, Google search!]
  2. Open
http://zpzvnnuvtzsfv3t2senkmib3zr6xen7zbvnzy3ted75sf4cvkw3eg5qd.onion/914b65db8aa50d86fddfc979ce4c445ef49e0874f73560e5e4bc6eaeb5c804d3b33d6f489328bd7a323ddce5d1bcc690/
>>> Warning! Recovery recommendations.
 Do not MODIFY or REPAIR your files, Or they will be lost forever.
 Do not hire a recovery company.Can't solve anything without us,They always think they're expert negotiators, but the truth is they don't care about you and business
 Do not report to the Police, FBI,They don't care about your business and it's going to get worse.(You could be hit with a hefty fine.)
```

[Knight 랜섬노트]



RansomHub.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
Hello!

Visit our Blog:

Tor Browser Links:
        http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
         http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by
your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.


>>> If you have an external or cloud backup; what happens if you don't agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies
and the data of your company's customers will be published on the internet, and the respective country's personal data usage authority will be informed. Moreover,
confidential data related to your company will be shared with potential competitors through email and social media. You can be sure that you will incur damages far
exceeding the amount we are requesting from you should you decide not to agree with us.


>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look
incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP
legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>, The government uses your fine to reward them.And you will not get anything, and except
you and your company, the rest of the people will forget what happened!!!!!


>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://hqnonbqw5wqg4xuzqi3ixigb3pamhjvdmmsrvm6me4rtn3kikdiy7oid.onion/
- Log in using the Client ID: 9b483acd0e95288cbe42aaa8e51afc8744405e7cca20a45f78ba8a03c6f469


>>> WARNING

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
```

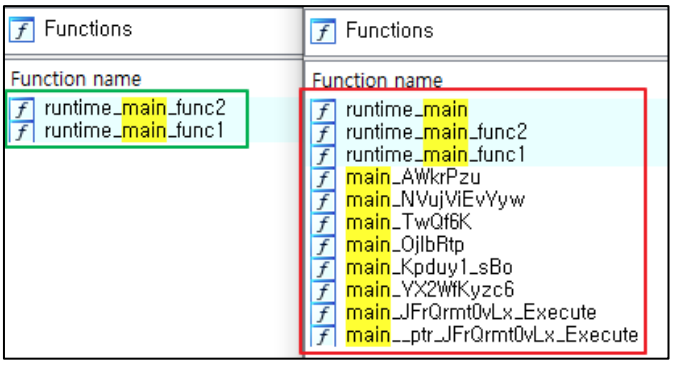
[RansomHub 랜섬노트]

✓ 기능 분석

1) 분석 체크 사항

- 심볼 복원

RansomHub는 Go 언어로 제작되어 기본적으로 분석에 많은 시간이 소요된다. 여기에 추가로 함수 이름, 변수 등을 확인할 수 있는 심볼이 숨겨져 있어 해당 심볼을 찾아 적용 후 분석을 진행한다. 디스어셈블러를 통해 살펴보면 심볼을 불러오지 못한 경우와 심볼 값을 불러왔을 때의 차이를 확인할 수 있다. Go 언어로 제작된 경우 보통 main(혹은 특정 클래스 이름)으로 시작하는 함수 이름에서 주요 기능을 수행한다.



[심볼 적용 전/후 비교]

- 문자열 동적 로드

탐지 회피와 분석 방해를 목적으로 실행에 필요한 문자열, 명령어 등을 고유한 키와 연산을 통해 동적으로 디코딩 후 사용한다.

```
v25 = m_getstring_sub_6ED8C0();               // powershell.exe
v4 = m_getstring_sub_6ED9C0(a1, a2);          // -Command
key = 0x47C7A2453A4E9F8BLL;
v20 = 0x77E3;
encoded = 0xAC2FF5B79FC50EDBLL;
v18 = 0xE34F;
for ( i = 0LL; i < 0xA; ++i )
{
  Powershell_str = *(&key + i);
  a2 = *(&encoded + i) - Powershell_str;
  *(&encoded + i) -= Powershell_str;
}
v24 = v4;
v7 = runtime_slicebytetostring(a1, a2, Powershell_str, 0xALL);// PowerShell
```

[문자열 동적 로드]

- -pass 키

64자리 값을 실행 시 -pass 키로 전달해야 정상적으로 실행되며 전달된 pass 키는 랜섬웨어 실행에 필요한 설정값을 복호화 하는데 사용된다.

2) 기능 상세 분석

- **Config load**

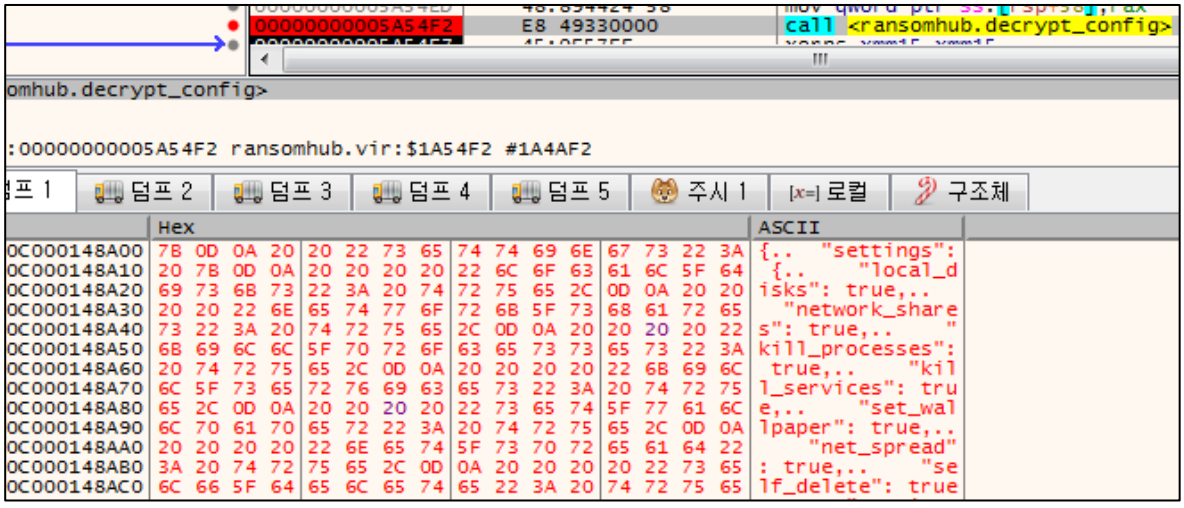
pass 인자로 전달된 키를 이용해 설정값을 복호화 후 정상적인 값이 확인되지 않으면 "bad config"를 출력 후 종료된다. 해당 샘플의 분석은 공격에 사용된 키를 사용하지 않고 정상적으로 사용된 설정값을 디버거를 통해 메모리 패치 후 분석을 진행했다.

```
config_error = *(qword_9A6798 + 8);
v9 = decrypt_config();                          // key check & decrypt config(json)
if ( dword_9FCA50 )
{
  v5 = &qword_9A6780;
  runtime_gcWriteBarrier();
}
else
{
  qword_9A6780 = v9;
}
if ( config_error )
{
  m_get_string_0();                             // load string "bad config"
  v270 = v3;
  v43 = runtime_convTstring();
  *&v270 = &type__ptr_string;
  *(&v270 + 1) = v43;
  m_console_print(1LL, 1LL);
  runtime_deferreturn(1LL, 1LL, v44, v45, v46, v47, v198);
  return;
```

[Config 체크 로직]

```
C:₩Sample>RansomHub.exe -pass testkey
bad config
```

[Config 로드 실패 시 출력]



[Config 값 메모리 패치]

- **Sleep (Opt.)**

실행 시 -sleep 인자를 사용하면 설정값을 로드 후 지정한 시간만큼 프로그램 실행을 멈춘다.

```
if ( *sleep_time > 0 )
{
  v244 = sub_729220();                          // sleep %d minute to encryption
  v216 = 0LL;
  v269 = v3;
  v10 = runtime_convT64();
  *&v269 = &type__ptr_int;
  *(&v269 + 1) = v10;
  v5 = v216;
  a2 = &v269;
  olMJKnrSuq_Bzo6TNVJEyrs();
  m_get_sleep(v5, &v269);
}
```

[-sleep 동작 로직]

- **Mutex (Config Opt.)**

설정값의 "settings"-"running_one" 값이 true로 설정되어 있을 경우 "mutex_{master_public_key}" 형태로 Mutex[25]를 생성한다.

```
if ( *(qword_9A6780 + 0x17) )                   // running_one
{
  rand_str = sub_729B00();                      // mutex_%s
  v236 = 0LL;
  v271 = v3;
  v16 = runtime_convTstring();
  *&v271 = &type__ptr_string;
  *(&v271 + 1) = v16;
  v17 = v236;
  sub_563020(1LL, 1LL, v18, &v271);             // mutex_{master_public_key}
  m_string_to_urf16(1LL);
  if ( !v17 )
    sub_459D40(1LL, 1LL, v20, 0LL, v21, v22, v198);
  v265 = v19;
  m_openmutex(1LL, 1LL, v20, v19);              // OpenMutex
  m_createmutex();                              // CreateMutex
```

[Mutex 설정]

[25] Mutex : 중복 실행을 방지하기 위한 동기화 메커니즘

- **White host 확인 (Config Opt.)**

설정값의 "white_hosts"가 설정되어 있으면 더 이상 실행되지 않고 프로그램을 종료한다.

```
if ( v50 == v234 && m_white_host_check(v14, v48, v51, v234) )
{
  sub_72A620(v14, v48);                         // white host
  v271 = v3;
  v52 = runtime_convTstring();
  *&v271 = &type__ptr_string;
  *(&v271 + 1) = v52;
  fXPY11eRA10__ptr_GH6mB3yf_Println(1LL);
  runtime_deferreturn(1LL, v48, v53, v54, v55, v56, v198);
  return;
}
```

[white host 체크]

- **Client ID 생성**

호스트 이름과 master_public_key를 통해 Client ID를 생성한다. Client ID는 랜섬노트에 기재되며, RansomHub 그룹과 협상할 때 로그인 ID로 사용된다.

```
hostname_str = m_hostname_sub_72A880(v14, v27);// hostname
v263 = runtime_stringtoslicebyte();
hostname_str_1 = hostname_str;
v235 = v58;
runtime_stringtoslicebyte();
v59 = qword_9A75A8;
v60 = v263;
hostname_str_2 = hostname_str_1;
client_id = m_create_client_id(v198, v201, v203);// 9b483acd
```

[Client ID 생성]

- **안전 모드 부팅 (Opt.)**

실행 시 -safeboot, -safeboot-instance 인자가 설정되어 있으면 안전 모드로 부팅해 프로세스가 진행된다. 우선 안전 모드 부팅을 위해 관리자 권한을 체크 후 권한이 없는 경우 CMSTPLUA(Component Management System Template) COM 객체[26] 취약점을 이용한 권한 상승을 시도한다.

```
if ( !v80 && !OpenProcessTokenOpenSCManagerW && !*qword_9A6770 )// administrator check
{
  if ( m_get_process_token(publickey, 1LL, v85) )
  {
    v86 = m_uac_bypass_run();                   // Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
```

[CMSTPLUA COM 객체 취약점을 이용한 권한 상승]

[26] CMSTPLUA COM 객체 : Windows에서 관리자 권한 없이도 특정 작업을 수행할 수 있게 해주는 계정 권한 상승 기능 제공 객체

부팅 시 자동 로그온을 사용하기 위해 DefaultUserName[27], DefaultDomainName[28], DefaultPassword[29] 레지스트리 값을 설정해 바로 부팅이 가능하도록 설정을 한다. 이름과 비밀번호는 Config의 "credentials" 값이 유효하면 해당 값으로 설정하고, 그렇지 않으면 동적으로 생성한 자격 증명을 NetUserSetInfo 함수를 통해 사용자 계정을 업데이트 후 사용한다. 사용한 로그인 정보는 랜섬웨어가 실행된 경로에 user.txt 파일로 기록된다.

```
m_user_logon(v199, v202, v204, client_id, v206, v207);// logon check
if ( !v111 )
{
  v80 = *(v239 + 8);
  v81 = *(v239 + 0x10);
  publickey = 0LL;
  if ( !m_regsetvalue_autologin(0LL, v81) )// SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName
                                           // SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultDomainName
                                           // SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultPassword
  {
    sub_72BB80();                          // fail: set user auto logon
```

<자동 로그온 설정>

안전 모드로 부팅 후 자동 실행되도록 RunOnce[30] 레지스트리 값을 설정 후 시스템을 재부팅한다.

```
v130 = m_set_RunOnce();                 // -safeboot-instance -pass {pass_key}
                                        // SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
if ( v130 )
{
  v221 = v130;
  v249 = v129;
  sub_72C7C0(5, 2LL);                   // unable to set safe boot run
  v273 = v3;
  v274 = v3;
  v131 = runtime_convTstring();
  *&v273 = &type__ptr_string;
  *(&v273 + 1) = v131;
  v132 = v221;
  if ( v221 )
    v132 = *(v221 + 8);
  *&v274 = v132;
  *(&v274 + 1) = v249;
  fXPY11eRA10__ptr_GH6mB3yf_Println(2LL);
  runtime_deferreturn(2LL, 2LL, v133, v134, v135, v136, v200);
}
else
{
  sub_72CB00();                         // wait 60s restart to safe mode
  v268 = v3;
  v137 = runtime_convTstring();
  *&v268 = &type__ptr_string;
  *(&v268 + 1) = v137;
  m_console_print(1LL, 1LL);
  m_get_sleep(1LL, 1LL);
  m_call_restart();
```

[자동 실행 설정 및 재부팅]

[27] DefaultUserName : 시스템에서 자동 로그인 기능을 설정할 때 사용자 이름을 저장하는 데 사용

[28] DefaultDomainName : 시스템에서 자동 로그인 기능을 설정할 때 네트워크 도메인 이름을 저장하는데 사용

[29] DefaultPassword : 시스템에서 자동 로그인 기능을 설정할 때 사용자의 비밀번호를 저장하는데 사용

[30] RunOnce : 시스템이 시작될 때 자동으로 한 번 실행될 프로그램이나 스크립트를 등록하는데 사용

- 네트워크 비활성화 (Opt.)

-disable-net 옵션이 설정된 경우 netsh.exe를 이용해 interface를 얻어온 후 disable 설정을 통해 네트워크를 비활성화한다.

```
v91 = m_get_net_interface(var1);              // get interface
v242 = v91;
v213 = v80;
v214 = v92;
if ( var1 )
{
  v238[0] = 0x4CC35774EC0F5C93LL;
  v238[1] = 0x5DB943558EA8AB93LL;
  v238[2] = 0x6FFE7BA1EE1F121CLL;
  v237[0] = 0x285D0EF8765212E2LL;
  v237[1] = 0x11B0DD1FD7BF75DCLL;
  v237[2] = 0x467E8C078535358LL;
  for ( i = 0LL; i < 0x18; ++i )
    *(v237 + i) += *(v238 + i);
  v251 = 1LL;
  v223 = var1;
  runtime_slicebytetostring(var1, 1LL, i, 0x18LL);// unable to get interfaces
```

```
while ( v80 > var1 )
{
  hostname_str_1 = var1;
  v264 = v91;
  m_netsh_interface(var1, v81, *v91, 0);    // netsh.exe interface set interface "interface name" disable
  v91 = v264 + 2;
  var1 = hostname_str_1 + 1;
  v92 = v214;
  v80 = v213;
  v81 = v242;
}
```

[네트워크 비활성화]

- 프로세스 및 서비스 종료 (Config Opt.) / 백업 및 이벤트 로그 삭제 / 윈도우 서버 중지

휴지통에 있는 파일로 복구를 하지 못하도록 파일을 삭제하고 윈도우 복원을 무력화하기 위해 볼륨 섀도 카피(VSC, Volume Shadow Copy)[31]를 제거한다. 또한, 사고 조사 및 흔적을 지우기 위해 윈도우 이벤트 로그를 삭제하며 윈도우 서버를 종료하는 명령어를 실행한다.

```
m_SHEmptyRecycleBinW();                 // delete recycle
if ( v3 )
{
  m_iisreset_stop();                    // cmd.exe /c iisreset.exe /stop
  m_remove_ShadowCopy();                // powershell.exe -Command "Get-CimInstance Win32_ShadowCopy | Remove-CimInstance"
  m_remove_event_log();                 // wevtutil.exe cl "security" & wevtutil.exe cl "system" & wevtutil.exe cl "application"
```

[명령어 및 커맨드 라인]

[31] 볼륨 섀도 카피 : Windows에서 파일이나 폴더의 백업 복사본을 생성하고 유지하는 기술

프로세스 및 서비스로 동작 중인 암호화 대상 파일을 모두 암호화하기 위해 프로세스 및 서비스를 종료하며, 가상 머신(VM)을 Powershell 명령어를 통해 중지한다.

카테고리	서비스 목록
백업 소프트웨어	mepocs, memtas, veeam, VeeamNFSSvc, VeeamDeploymentService, VeeamTransportSvc, AcronisAgent, AcrSch2Svc, BackupExecVSSProvider, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, GxBlr, GxVss, GxCIMgrS, GxCVD, GxCIMgr, GXMMM, GxVssHWProv, GxFWD, PDVFSService, MVArmor, MVarmor64, VSNAPVSS
데이터베이스	sql, sql$, mysql, mysql$, QBDBMgrN, QBIDPService, QBCFMonitorService
이메일 서버	MSExchange, MSExchange$, WSBExchange
보안 소프트웨어	Sophos, SAPService, SAP, SAP$, SAPD$, SAPHostControl, SAPHostExec

[서비스 종료 대상]

카테고리	서비스 목록
백업 소프트웨어	agntsvc.exe, BackupExecAgentAccelerator.exe, BackupExecAgentBrowser.exe, BackupExecDiveciMediaService.exe, BackupExecJobEngine.exe, BackupExecManagementService.exe, BackupExecRPCService.exe, bedbh.exe, vxmon.exe, benetns.exe, bengien.exe, pvlsvr.exe, beserver.exe, vsnapvss.exe, VeeamNFSSvc.exe, VeeamTransportSvc.exe, VeeamDeploymentSvc.exe, raw_agent_svc.exe, CVMountd.exe, cvd.exe, cvfwd.exe, CVODS.exe, avagent.exe, avscc.exe
데이터베이스	dbeng50.exe, dbsnmp.exe, sql.exe, sql.exe, sqbcoreservice.exe, QBDBMgrN.exe, QBIDPService.exe, QBCFMonitorService.exe, isqlplussvc.exe, ocautoupds.exe, ocomm.exe, ocssd.exe, oracle.exe
이메일/메신저	thebat.exe, thunderbird.exe, tbirdconfig.exe, outlook.exe, msaccess.exe
문서 소프트웨어	excel.exe, onenote.exe, powerpnt.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe, infopath.exe, mspub.exe
웹 브라우저	firefox.exe
관리 소프트웨어	saposcol.exe, saphostexec.exe, sapstartsrv.exe, SAP.exe, DellSystemDetect.exe, EnterpriseClient.exe, CagService.exe, mydesktopqos.exe, mydesktopservice.exe, xfssvccon.exe, synctime.exe, steam.exe
원격 제어	TeamViewer_Service.exe, TeamViewer.exe, tv_w32.exe, tv_x64.exe

[프로세스 종료 대상]

```
powershell.exe -Command PowerShell -Command "Get-VM | Stop-VM -Force"
```

[VM 중지 명령어]

- **Ransomnote 생성**

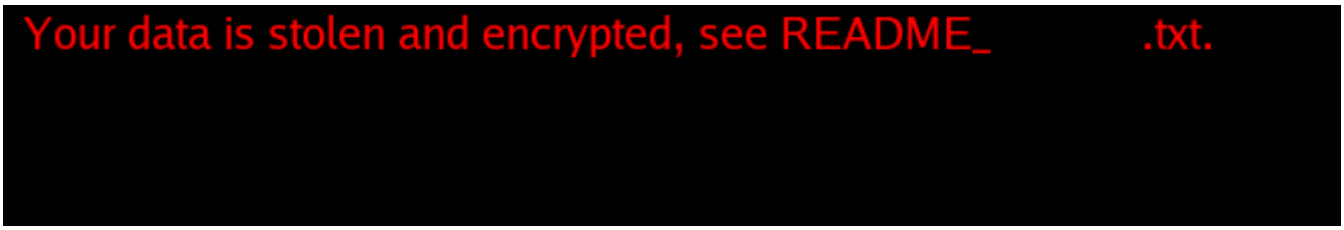
암호화 대상이 포함된 모든 디렉토리에 설정값에 명시된 파일명("note_file_name")과 내용("note_full_text")을 포함한 랜섬노트를 생성한다.

```
Hello!

Visit our Blog:

Tor Browser Links:
       http://ranso                                                    .onion/

Links for normal browser:
        http://ransom                                                    .onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by
your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.


>>> If you have an external or cloud backup; what happens if you don't agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies
and the data of your company's customers will be published on the internet, and the respective country's personal data usage authority will be informed. Moreover,
confidential data related to your company will be shared with potential competitors through email and social media. You can be sure that you will incur damages far
exceeding the amount we are requesting from you should you decide not to agree with us.


>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look
incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP
legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>, The government uses your fine to reward them.And you will not get anything, and except
you and your company, the rest of the people will forget what happened!!!!!


>>> How to contact with us?

- Install and run 'Tor Browser' from https://www.torproject.org/download/
- Go to http://hqno                                                    .onion/
- Log in using the Client ID: 9b                                                    69


>>> WARNING

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
```

[RansomHub 랜섬노트]

- **바탕화면 변경 (Config Opt.)**

설정값의 "note_short_text" 값을 이용해 검은색 배경의 {random}.png 파일을 생성 후 레지스트리 설정을 통해 바탕화면을 변경한다.



[바탕화면 변경]

- **파일 암호화**

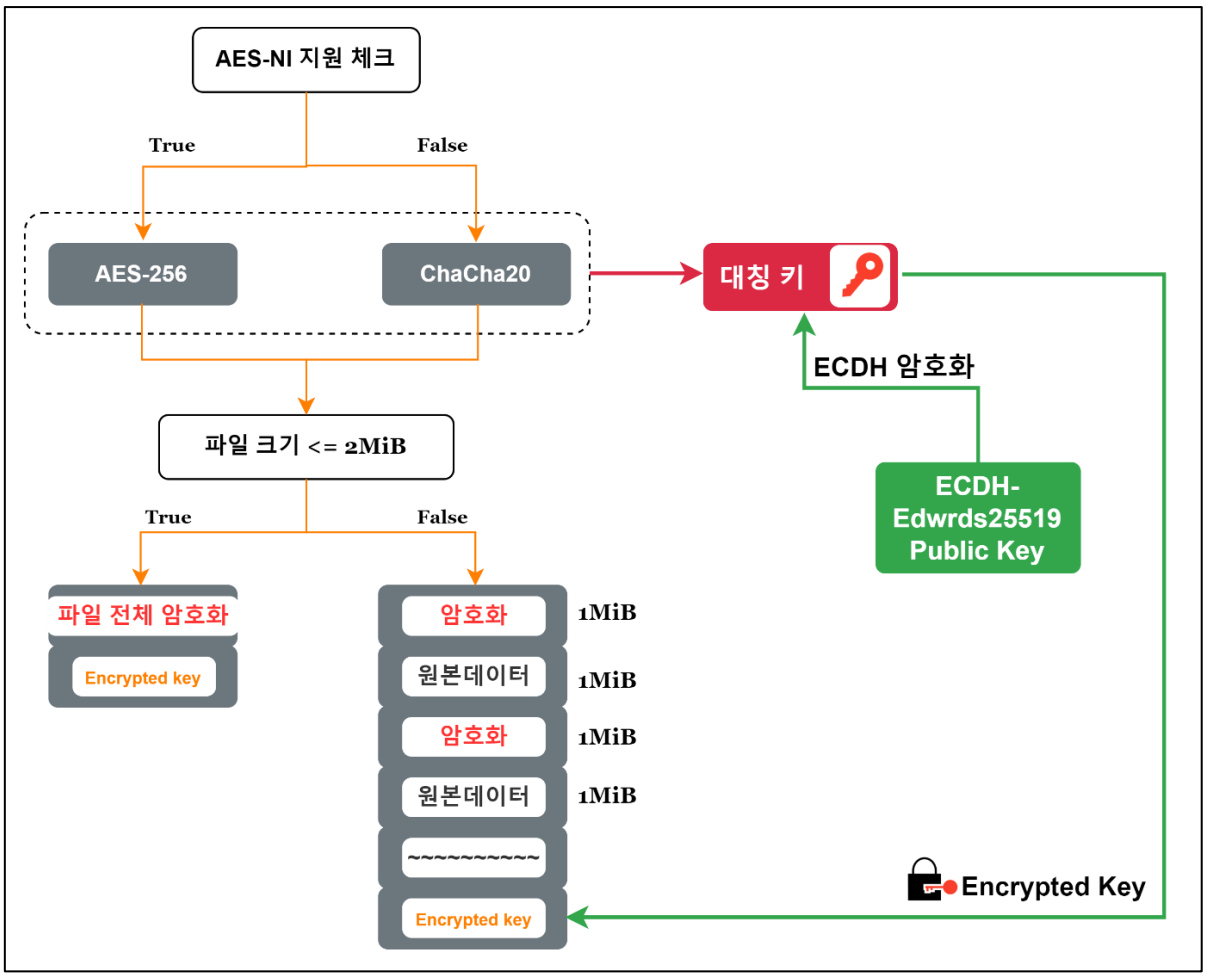
파일을 암호화하기 전에 Config에 명시되어 있는 암호화 제외 폴더(“white_folders”), 랜섬노트 이름(“note_file_name”), 제외할 파일명과 확장자(“white_files”)를 포함할 경우 암호화 대상에서 제외된다.

카테고리	서비스 목록
파일 이름	NTUSER.DAT, autorun.inf, boot.ini, desktop.ini, thumbs.db
확장자	*.deskthemepack, *.themepack, *.theme, *.msstyles, *.exe, *.drv, *.msc, *.dll, *.lock, *.sys, *.msu, *.lnk, *.ps1, *.iso, *.inf, *.cab, *.386
랜섬노트 이름	Config의 “note_file_name” 항목
폴더 이름	Root
	\$windows.~ws, *\$windows.~bt*, *\windows*, *\windows.old*, *\system volume information*, *\Boot*, *\PerfLogs*
	*\AppData
	\Local\Temp*, \Local\Microsoft\GameDVR*, \Local\Microsoft\Edge*, \Local\Packages\Microsoft.*, \Local\Packages\MicrosoftWindows.*, \Local\Packages\Internet Explorer*
	*\Program Files\
	\Common Files\microsoft shared*, \Common Files\Services*, \Common Files\System*, \Internet Explorer*, \ModifiableWindowsApps*, \Uninstall Information*, \Windows Defender*, \Windows Mail*, \Windows Media Player*, \Windows NT*, \Windows Photo Viewer*, \Windows Portable Devices*, \Windows Security*, \Windows Sidebar*, \WindowsApps*, \WindowsPowerShell*
	*\Program Files (x86)
	\Common Files*, \Common Files\Microsoft Shared*, \Common Files\Services*, \Common Files\System*, \Internet Explorer*, \Microsoft*Edge*, \Microsoft\Temp*, \Microsoft.NET*, \Windows Defender*, \Windows Mail*, \Windows Media Player*, \Windows Multimedia Platform*, \Windows NT*, \Windows Photo Viewer*, \Windows Portable Devices*, \Windows Security*, \Windows Sidebar*, \WindowsPowerShell*
	*\ProgramData
	\ssh*, \USOPrivate*, \USOShared*, \Package Cache*, \Microsoft\Device Stage*, \Microsoft\DeviceSync*, \Microsoft\Diagnosis*, \Microsoft\DiagnosticLogCSP*, \Microsoft\DRM*, \Microsoft\UEV*, \Microsoft\EdgeUpdate*, \Microsoft\Event Viewer*, \Microsoft\IdentityCRL, \Microsoft\MapData*, \Microsoft\MF*, \Microsoft\NetFramework*, \Microsoft\Network*, \Microsoft\Provisioning*, \Microsoft\Search*, \Microsoft\SmsRouter*, \Microsoft\Spectrum*, \Microsoft\Speech_OneCore*, \Microsoft\Storage Health*, \Microsoft\User Account Pictures*, \Microsoft\Vault*, \Microsoft\WDF*, \Microsoft\Windows*, \Microsoft\Windows Defender*, \Microsoft\Windows NT*, \Microsoft\Windows Security Health*, \Microsoft\WinMSIPC*, \Microsoft\WPD*, \Packages\USOPrivate*, \Packages\USOShared*, \Packages\WindowsHolographicDevices*, \Packages\MicrosoftWindows.*, \Packages\Microsoft.*

[암호화 제외 대상]

실행 시 설정한 옵션에 따라 암호화 대상이 구분되며 -host 옵션은 SMB host를 암호화 대상으로 선정하고, -only-local 옵션은 로컬 디스크만을 대상으로 암호화한다. 또한 -path 옵션을 사용할 경우 지정한 경로 혹은 SMB host의 경로를 지정해 암호화가 가능하다. Config의 “network_shares” 값이 true이면 네트워크 공유 폴더 또한 암호화되고,

"net_spread" 값이 true인 경우 SMB를 통한 전파 기능을 수행한다.



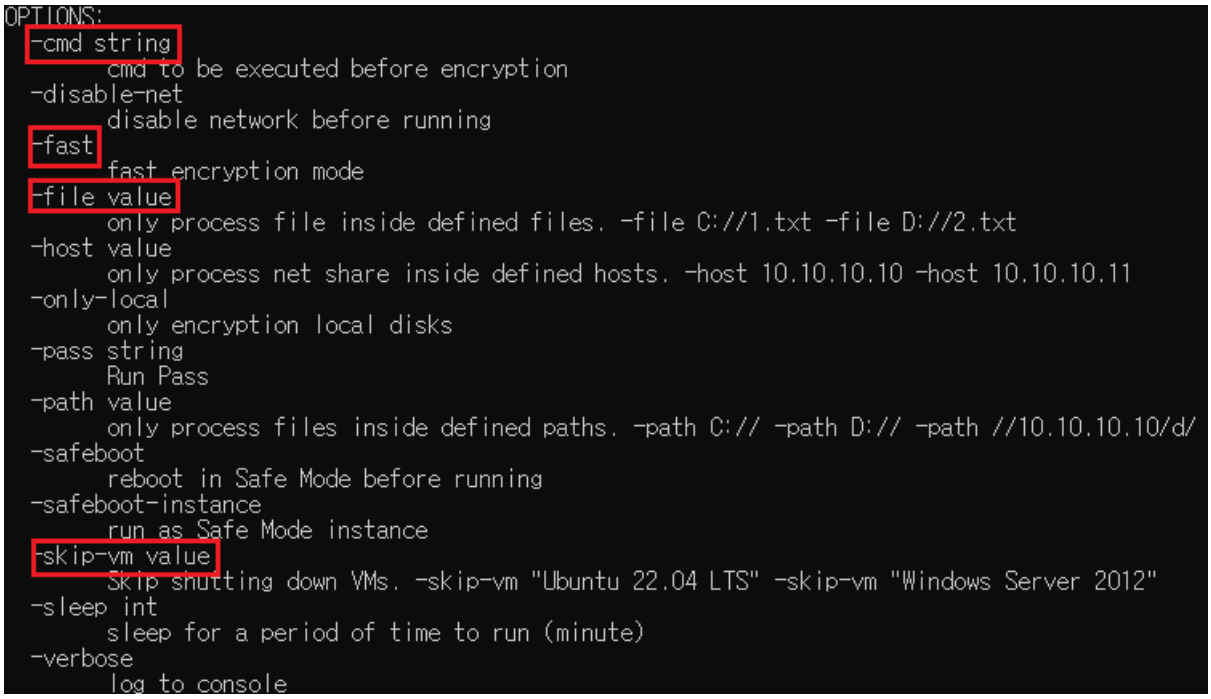
[암호화 로직]

RansomHub가 사용한 암호화 알고리즘은 대칭키 암호인 AES-256, ChaCha20과 비대칭키 암호 ECDH-Edwards25519 알고리즘을 사용했다. 파일을 암호화할 때 AES-NI[32] 지원 여부를 체크하고 지원이 가능하면 AES 암호화 알고리즘을 사용하며, 지원하지 않을 경우 AES 보다 암호화 속도가 빠른 ChaCha20 알고리즘을 사용했다. 보통의 경우 ChaCha20이 빠르지만 AES-NI는 하드웨어를 통한 가속이 가능해 이와 같은 방식을 채택한 것으로 보인다. 파일 암호화에 사용한 키는 ECDH-Edwards25519 비대칭키 암호화 알고리즘을 사용해 보호한다. 암호화된 키는 암호화 과정이 끝난 파일의 끝부분에 기록해 저장한다.

RansomHub는 빠른 암호화 속도를 지원하기 위해 파일 크기에 따라 부분 암호화 방식을 채택하고 있는데 파일 크기가 2MiB($2 * 10^6$ Byte) 이하일 경우 파일 전체를 암호화하며, 초과하는 경우 1MiB(10^6 Byte) 단위로 암호화한다. 즉, 암호화된 1MiB + 원본 데이터 1MiB + 암호화된 1MiB + 원본 데이터 1MiB 형태로 반복하는 구조를 가지고 있다. 파일 암호화가 끝나면 파일명 뒤에 Config에 명시된 확장자("extension")를 추가한다.

[32] AES-NI : 고속화된 데이터 암호화 및 복호화를 가능하게하여 AES 알고리즘의 성능을 향상 시키는 명령어 세트

3) 기능 업데이트



[업데이트 후 인자 목록]

가장 최근에 발견된 RansomHub 랜섬웨어에서 몇 가지 기능이 추가됐다. 기능적으로 크게 차이 나는 사항은 없으며, 눈여겨볼 특징은 크게 두 가지다. 첫 번째는 인자가 몇 개 추가됐는데, -fast 모드에서는 파일 사이즈와 관계없이 2MiB 이상 파일을 처리하는 방식과 동일하게 부분 암호화를 수행한다. -cmd 인자로는 암호화 전에 실행할 명령어를 따로 지정할 수 있으며, 지정된 파일만 암호화하는 -file 인자도 추가됐다. 마지막으로 VM 이름을 "Ubuntu 22.04 LTS"와 같이 명시하면 해당 VM은 종료하지 않는 기능도 추가됐다.

두 번째는 사용자의 언어를 화이트 리스트 방식으로 검사하여 리스트에 포함될 경우 랜섬웨어가 실행되지 않고 종료된다는 특징이 있다.

비교 언어 목록
우크라이나어, 러시아어, 루마니아어, 히브리어, 아르메니아어, 베트남어, 타지크어, 벨라루스어, 카자흐어, 조지아어, 마케도니아어, 아제르바이잔어, 중국어, 우즈베크어, 투르크멘어, 키르기스어

옵션에 따라 제공하고 있는 기능에 대한 상세 설명은 다음 표와 같다. 추가된 옵션은 음영처리되어 있는 cmd, fast, file, skip-vm 옵션이다.

인자	기능 설명
-cmd string	암호화 전에 실행할 명령어 지정
-disable-net	실행 전 네트워크 비활성화
-fast	빠른 암호화 모드 실행
-file value	지정된 파일만 암호화
-host value	지정된 호스트 내의 공유 자원 암호화

-only-local	로컬 디스크만 암호화
-pass string	설정 값 복호화 키
-path value	지정된 경로 내의 파일만 암호화
-safeboot	실행 전에 안전 모드로 부팅
-safeboot-instance	안전 모드일 경우에 실행
-skip-vm value	지정된 VM 은 종료하지 않음
-sleep int	지정된 시간(분) 동안 실행 대기
-verbose	콘솔에 로그 기록

[인자별 수행 기능 목록]

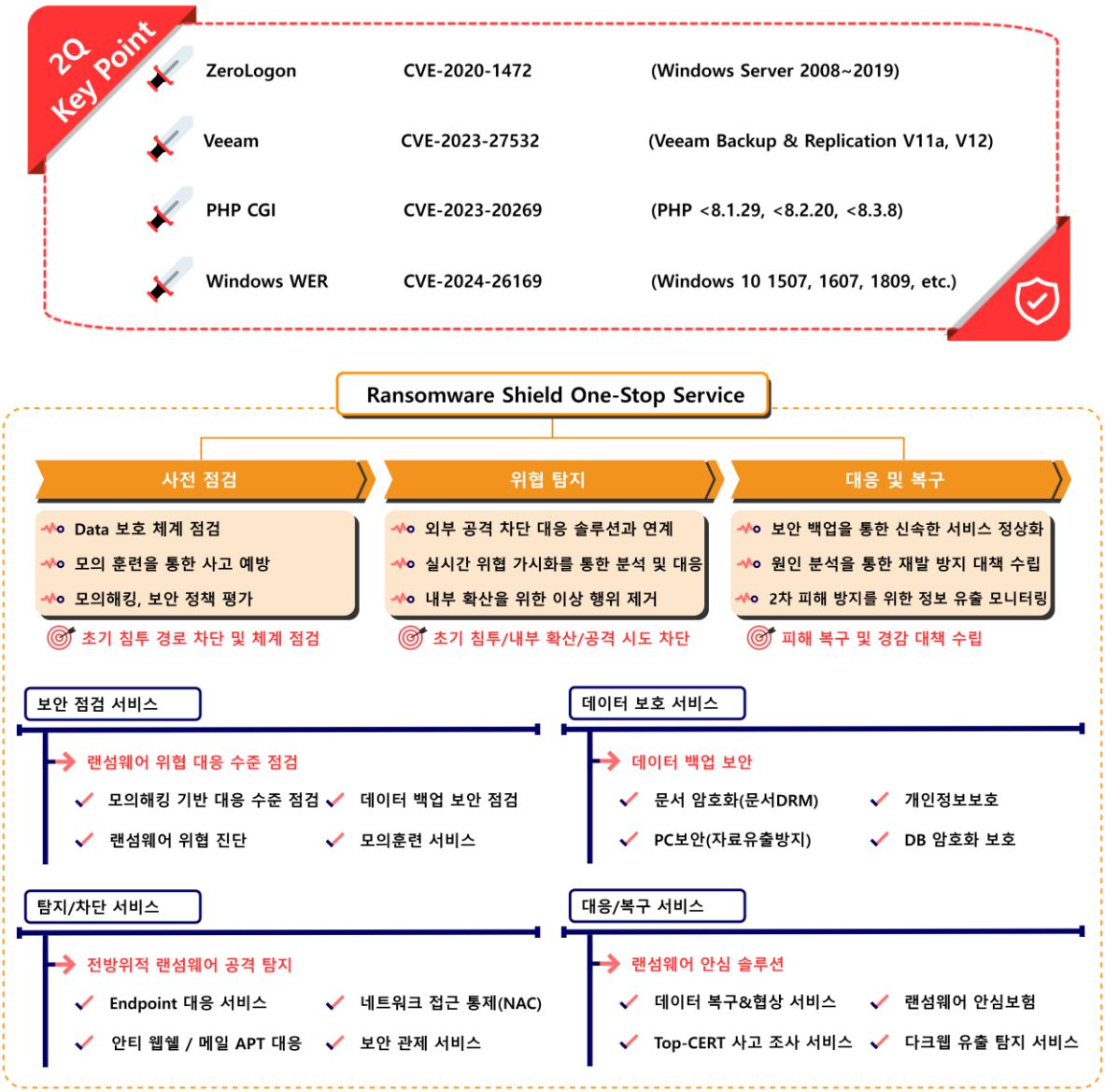
4. IoCs

First Seen	SHA256
2024-02-28	8F59B4F0F53031C555EF7B2738D3A94ED73568504E6C07AA1F3FA3F1FD786DE7
2024-03-12	34E479181419EFD0C00266BEF0210F267BEAA92116E18F33854CA420F65E2087
2024-03-31	7539BD88D9BB42D280673B573FC0F5783F32DB559C564B95AE33D720D9034F5A
2024-04-04	36E5BE9ED3EC960B40B5A9B07BA8E15D4D24CA6CD51607DF21AC08CDA55A5A8E
2024-04-06	02E9F0FBB7F3ACEA4FCF155DC7813E15C1C8D1C77C3AE31252720A9FA7454292
2024-04-10	EA9F0BD64A3EF44FE80CE1A25C387B562A6B87C4D202F24953C3D9204386CF0
2024-07-17	342B7B89082431C1BA088315C5EE81E89A94E36663F2AB8CFC27E17F7853CA2B
2024-07-22	56856E1E275CEBCD477E3A2995CD76398CFBB6C210181A14939C6307A82E6763
2024-07-25	83654C500C68418142E43B31EBBEC040D9D36CFBBE08C7B9B3DC90FABC14801A

랜섬웨어 Mitigations

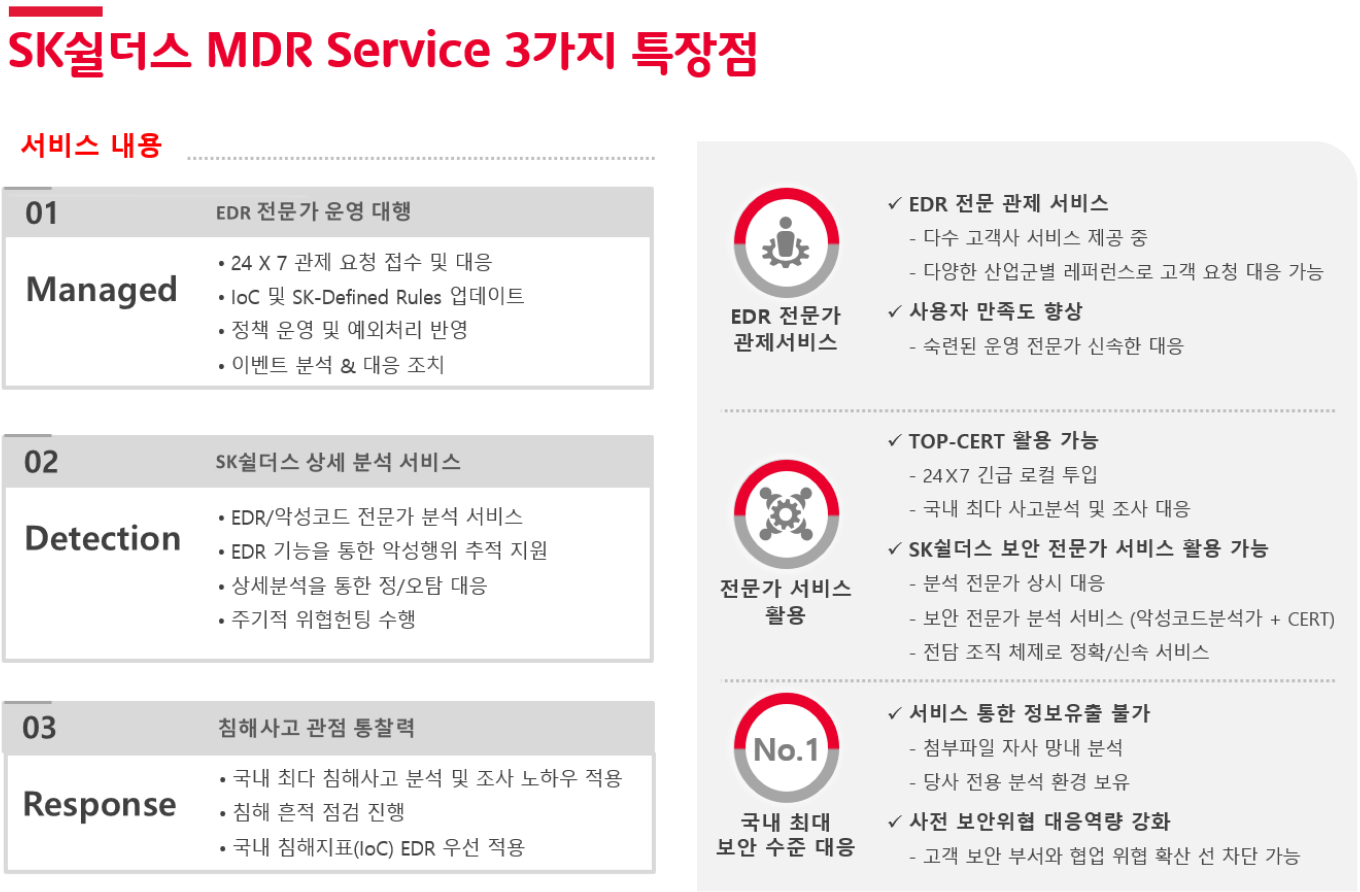
1. RansomHub 랜섬웨어 대응방안 안내

RansomHub 랜섬웨어는 취약점을 통해 초기 침투를 수행하는 것으로 관찰되었는데, 서비스형 랜섬웨어인 RaaS(Ransomware as a Service)로 운영되는 만큼 다양한 계열사를 보유하고 있어 여러 경로로 공격을 수행할 가능성이 높아 주의가 필요하다. 초기 침투 이후에도 다양한 RMM 도구와 네트워크 스캐닝 도구를 통해 지속성을 유지하고 내부 시스템에 전파되는 등의 악성 행위를 수행한다. 따라서 개인 사용자와 기업 사용자 모두 최소한의 보안 대책은 수립해 적용해야 한다. 무엇보다 초기 침투를 예방하는 것이 가장 중요하므로 시스템에 존재하는 잠재적인 위협을 진단하고 운영중인 시스템을 최신 버전으로 유지해야하며, 구성원들의 보안 인식을 제고할 수 있는 모의 훈련을 실시하는 방안이 필요하다. 이후에 발생할 수 있는 피해에 효과적으로 대응하기 위해서 전문 백업 서비스와 랜섬웨어 안심 보험 및 다크웹 유출 탐지 서비스를 고려할 것을 제안한다.

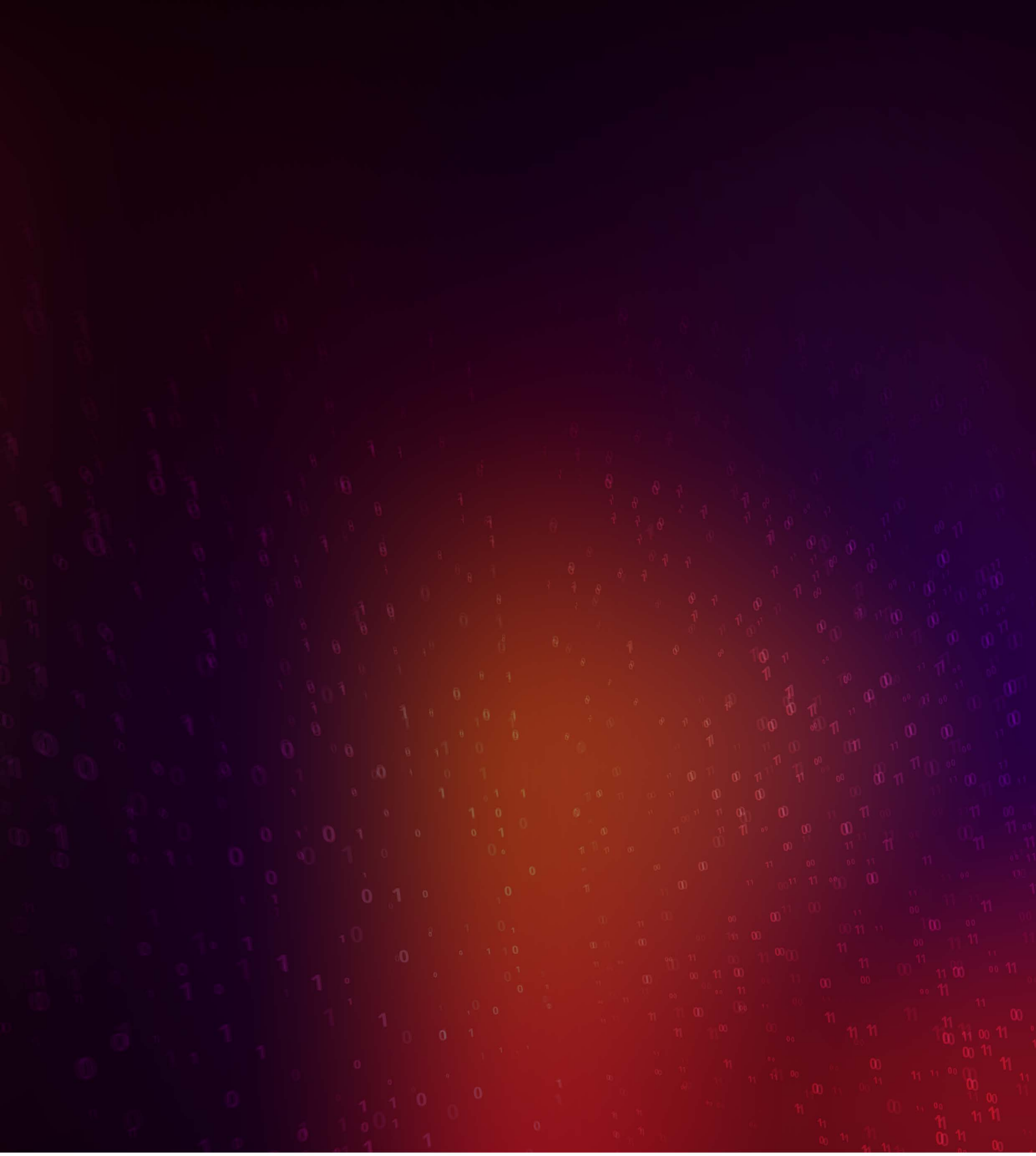


2. SK쉴더스 MDR 서비스

랜섬웨어에 전문적으로 대응하기 위해서 SK 쉴더스의 MDR(Managed Detection and Response) 서비스[33]를 사용하는 것이 효과적인 방안이 될 수 있다. 최근 랜섬웨어 공격자들의 치밀한 전략과 고도화된 탐지 회피 기법으로 인해 기존의 방어 체계만으로는 위협에서 벗어나기 어려운 상황이다. 이를 해결하기 위해 SK 쉴더스는 실시간으로 네트워크를 모니터링하고 이상 징후를 감지하며 필요시 즉각적으로 대응할 수 있는 MDR 서비스를 제공하고 있다. 랜섬웨어 공격은 사전 예방이 무엇보다 가장 중요하지만, 피해가 발생했을 경우 신속한 조치를 통해 피해를 최소화하는 것 또한 매우 중요하다. 따라서 기업에서는 전담 조직의 신속하고 정확한 사고 조사와 분석을 토대로 맞춤형 보안 솔루션을 제공하는 SK 쉴더스의 MDR 서비스를 고려하는 것을 추천한다.



[33] MDR 서비스 : 실시간 위협 감지와 대응을 통해 사이버 공격으로부터 조직을 보호하는 관리형 보안 서비스



안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 EQST/SI솔루션사업그룹 & KARA(Korea Anti Ransomware Alliance)
제　작 : SK쉴더스 마케팅그룹