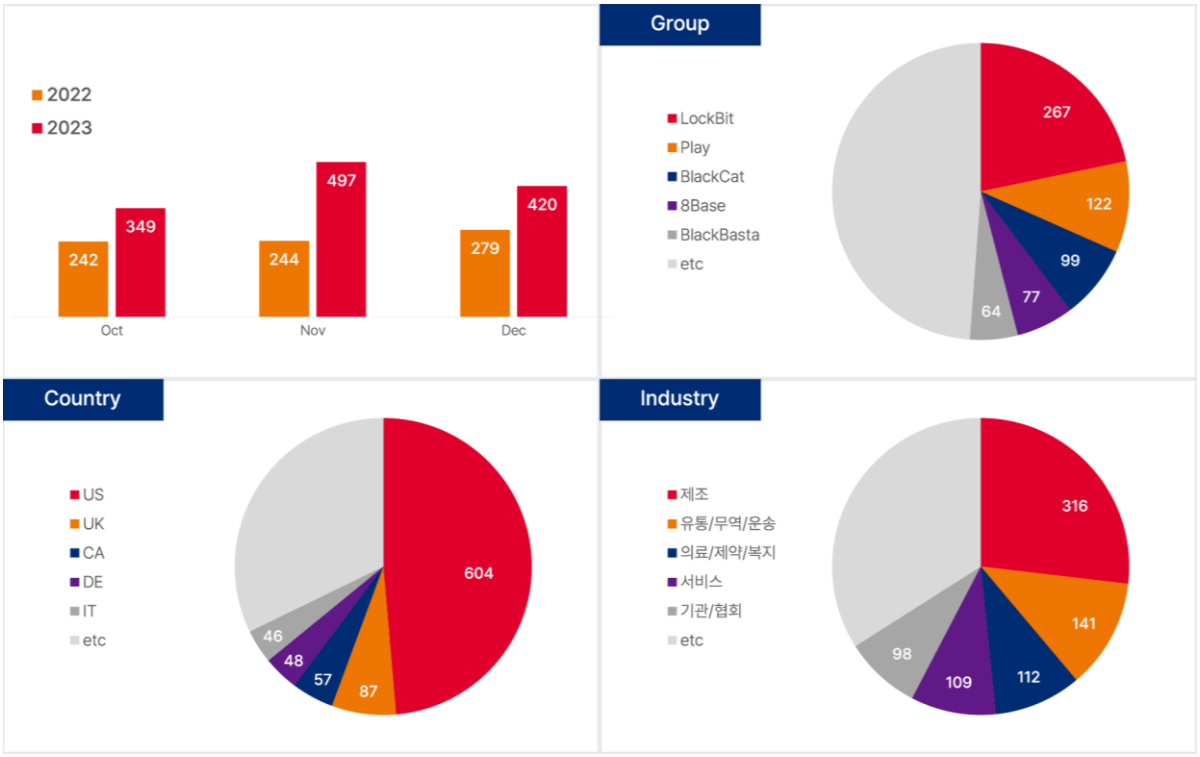
KARA
Korea Anti Ransomware Alliance

2023.4Q

KARA 랜섬웨어 동향 보고서

KARA 랜섬웨어 동향 보고서

랜섬웨어 트렌드



[그림 1] 4분기 랜섬웨어 활동 통계

4분기에는 지난 분기에 비해 9% 감소한 1,266건의 피해 사례가 확인되었다. 이는 지난 2분기 소프트웨어 취약점을 통해 대규모 공격을 수행한 Clop 그룹의 데이터 유출이 3분기까지 이어졌으나, 4분기에는 Clop 그룹의 활동량이 감소함과 동시에 Trigona, RagnarLocker, RansomedVC, NoEscape, BlackCat 랜섬웨어 그룹들의 폐쇄 혹은 운영상의 문제로 인한 결과로 볼 수 있다. LockBit 그룹은 12월 NoEscape, BlackCat 그룹의 운영 및 폐쇄 이슈가 발생하자 다크웹 포럼에 NoEscape, BlackCat 그룹의 계열사와 랜섬웨어 개발자를 포섭하려는 글을 게시하기도 했다.

4분기에 발생한 1,266건 중 약 10%는 새롭게 활동을 시작한 Hunters, WereWolves, DragonForce, SiegedSec, Raznatovic, Meow, Malek Team, Soldiers of Solomon 8개의 그룹에 의해 발생하였으며 그 중 정치, 사회적 목적을 달성하기 위한 핵티비즘 그룹인 Soldiers of Solomon 그룹이 랜섬웨어를 사용하는 모습도 확인되었다.

최근 랜섬웨어 그룹은 소프트웨어 취약점을 악용해 랜섬웨어 공격을 수행하는 전략을 선호하는 추세를 보이고 있으며 취약점을 악용한 공격은 하나의 취약점을 통해 여러 피해자를 대상으로 공격이 가능하며 패치되지 않은 대상을 선정하여 비교적 쉽게 접근이 가능하여 지속적으로 공격에 악용되고 있다.

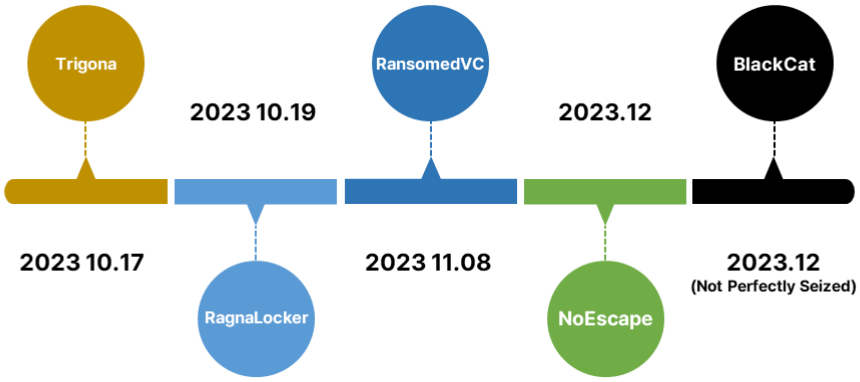
마지막으로 국내 기업의 피해 사례를 다크웹에서 분석한 결과 4분기에는 총 4건의 국내 피해 사례가 확인되었다. 10월 NoEscape 그룹에 의한 석유 제조 업체 감염, 11월 LockBit, Qilin 그룹에 의한 국제 기구 및 전자부품 제조 업체 감염, 12월에는 BlackSuit 그룹의 공격으로 골프관련 소프트웨어 개발 업체의 개인정보가 유출되었으며 유출된 데이터의 사용자를 대상으로 사칭 문자가 유포되어 2차적인 피해가 생길 수 있는 공격이 발생하였다. "그동안 우리 회사를 이용해 주심에 감사합니다. 서버 문제로 인한 죄송함을 담아 소수 회원님에게 자사주 3주(27만원 상당)를 선물로 드리고 있습니다. 수령을 원하시는 회원님은 답장으로 '수령'이라고 남겨주시면 빠른 기한 내로 직원이 연락드려 친절한 도움 드리겠습니다"라는 내용의 피싱 문자로 관련 문자를 받은 경우 발신번호를 스팸처리 하여 피해가 발생되지 않도록 주의를

기울여야 한다.

✓ 랜섬웨어 트렌드

1. 랜섬웨어 그룹의 잇단 폐쇄

4분기에는 랜섬웨어 그룹이 FBI[1], Europol[2], JIT[3]와 같은 국제 기관의 협력으로 폐쇄되거나, 수사기관의 압박으로 인해 운영을 중단한 사례가 확인되었다. Trigona, RagnarLocker, RansomedVC, NoEscape, BlackCat 그룹이 그 예이다.



[그림 2] 폐쇄 및 운영 중단 그룹

10월 17일 친 러시아 성향을 띄고 있는 Trigona 그룹이 우크라이나 사이버 동맹(UCA, Ukrainian Cyber Alliance)에 의해 폐쇄되었다. 이틀 후인 10월 19일에는 RagnarLocker 그룹 또한 Europol에 의해 폐쇄되었다. 한편 RansomedVC 그룹은 11월 8일 그룹의 관계자 6명이 체포되었고 98개의 계열사를 해고했다는 소식을 전하고 활동을 중단했다. 체포 소식이 있기 전 10월 30일, RansomedVC 그룹은 프로젝트를 팔고 싶다는 소식을 다크웹 포럼과 텔레그램 메신저를 통해 알렸는데 수사에 대한 압박을 지속적으로 받고 있었으며, 미숙한 운영으로 인한 계열사의 체포 또한 많은 영향을 미친 것으로 보인다.

한편 12월에는 NoEscape, BlackCat 그룹의 데이터 유출 사이트가 폐쇄되었다. NoEscape 그룹은 계열사가 "운영자가 수백만 달러의 몸값을 가져가고 유출사이트를 폐쇄시켰다"라고 진술해 운영자가 Exit scam[4]을 한 것으로 추측되고 있다. BlackCat 그룹은 12월 7일, 데이터 유출 사이트가 중단된 후 수사기관에 의한 폐쇄 의혹이 시사됐으나 BlackCat 그룹의 관리자가 하드웨어 오류로 인해 발생한 중단으로 곧 운영을 재개할 것이라고 언급했다. 12월 19일 BlackCat 그룹의 사이트에 FBI의 압수 포스터가 게재되며 그룹의 폐쇄가 이루어지는 듯했으나 같은 날 BlackCat 그룹은 데이터 유출 사이트를 복구 후 보복의 일환으로 미국 및 관련 기관에 대한 공격을 계열사들에게 허용하겠다는 글을 게시했다. 이후 데이터 유출 사이트는 계속해서 폐쇄, 복구되며 FBI와 BlackCat 그룹의 신경전이 이어졌으나 BlackCat 그룹은 데이터 유출 사이트를 다시 개설한 뒤 새로운 피해자들을 게시하고 있다.

이 외에도 12월에는 우크라이나에서 Dharma, Hive, LockerGoga, MegaCortex 등의 랜섬웨어를 사용한 그룹의 총책

---

[1] FBI(Federal Bureau of Investigation): 미국 법무부 산하의 수사 기관이자 정보 기관

[2] Europol: 유럽 연합의 범죄 대책 기구

[3] JIT(Joint Investigation Team): 유럽의 국가 수사 기관들이 공동으로 설립한 합동 수사 팀

[4] Exit scam: 대금을 받은 뒤 사업을 중단하는 사기유형

으로 의심되는 5명이 Europol 및 JIT의 협력을 통해 체포되는 등 국제 수사기관들의 협력으로 인해 랜섬웨어 그룹들이 폐쇄되는 사례가 확인되고 있다.

2. 핵티비즘 그룹의 랜섬웨어 활동

4분기에는 다수의 랜섬웨어 그룹이 활동하기 시작했다. 그 중에서도 GhostSec, Soldiers of Solomon 등 핵티비즘 그룹에 의한 랜섬웨어 활동이 발견되기도 했으며 하마스-이스라엘 전쟁의 일환으로 하마스 핵티비즘 단체에서 BiBi-Wiper[5]를 사용한 공격도 확인되었다.

그 중 GhostSec는 과거 이슬람 극단주의 단체 ISIS에 사이버 공격을 수행하기 위한 그룹으로, 2023년 10월 8일부터 텔레그램 메신저를 통해 GhostLocker 서비스형 랜섬웨어[6]를 판매하기 시작했다. 현재 GhostLocker의 제휴 가격은 999달러이며, 추후 4,999달러까지 인상할 계획이라고 밝혔다. 또한 Soldiers of Solomon 그룹은 친 팔레스타인 핵티비즘 그룹으로, 이스라엘의 기업 및 업체를 주 타깃으로 공격을 수행하고 빠르게 전파가 가능한 X(트위터)와 같은 SNS 채널 및 텔레그램 메신저를 통해 그룹의 행보를 알리고 있으며, 탈취한 데이터는 다크웹 포럼을 통해 유출하고 있다. 특히 이들은 Crucio라는 서비스형 랜섬웨어를 사용해 공격을 수행하는 것으로 알려져 있다.

3. 취약점을 악용한 랜섬웨어 공격

4분기에 공격에 악용된 취약점과 랜섬웨어 그룹은 'Apache ActiveMQ[7] / HelloKitty', 'Atlassian Confluence[8] / Cerber', 'SysAid[9] / Clop', 'Critix NetScaler[10] / LockBit', 'Qlik Sense[11] / Cactus' 이며, 이러한 공격을 막기 위해서 취약한 버전의 소프트웨어를 즉시 조치할 필요가 있다.

랜섬웨어	취약점 대상	취약점 번호	패치 여부
HelloKitty	Apache ActiveMQ	CVE-2023-46604	O
Cerber	Atlassian Confluence	CVE-2023-22518	O
Clop	SysAid	CVE-2023-47246	O
LockBit	Critix NetScaler	CVE-2023-4966	O
Cactus	Qlik Sense	CVE-2023-41265 CVE-2023-41266 CVE-2023-48365	O

표 1. 취약점을 악용한 랜섬웨어 공격

[5] BiBi-Wiper: 하마스 핵티비즘 단체에서 이스라엘의 기업들을 타겟으로 사용하는 데이터 삭제 악성코드

[6] 서비스형 랜섬웨어: RaaS(Ransomware-as-a-Service)라는 의미로, 돈을 주고 랜섬웨어를 제공받는 서비스

[7] Apache ActiveMQ: 송신자와 수신자 간의 메시지를 안전하게 전달하고 관리하는 오픈소스 소프트웨어

[8] Atlassian Confluence: 문서를 중앙화 하여 관리할 수 있는 협업 소프트웨어

[9] SysAid: 조직 내에 IT 서비스를 관리하기 위한 IT 서비스 관리 솔루션

[10] Critix NetScaler: 서버와 SQL 데이터베이스 트래픽을 관리하고 보완하는 네트워킹 플랫폼

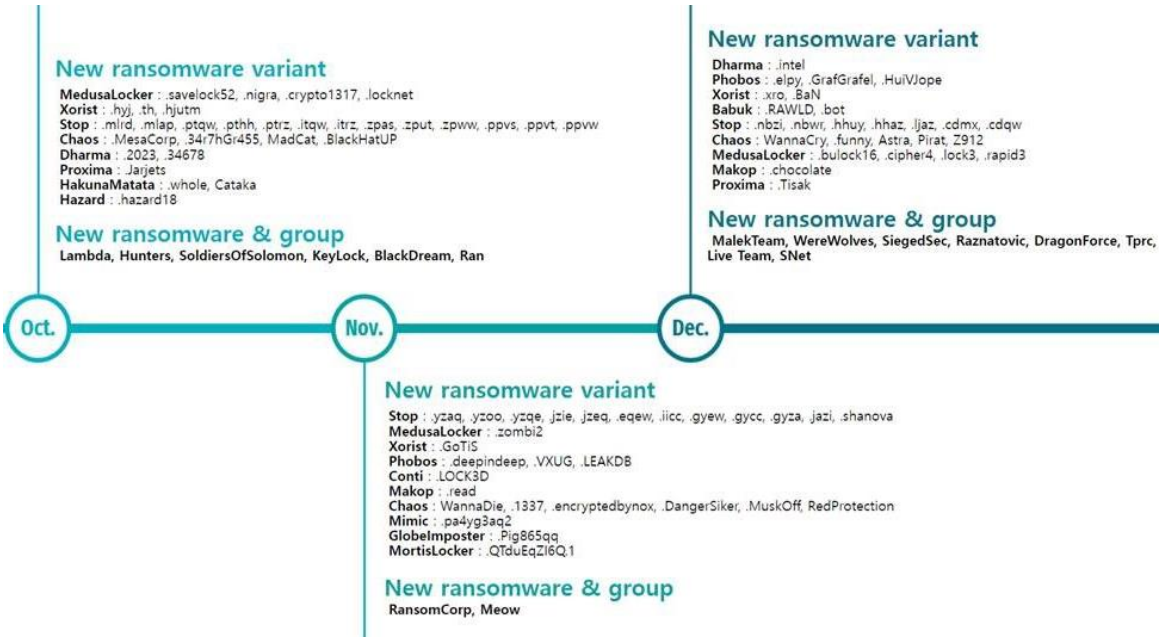
[11] Qulk Sense: 데이터 시각화 및 분석을 위한 플랫폼 또는 솔루션

4. Ransomware with ChatGPT

11월 말, 중국에서 랜섬웨어 공격자 4명이 체포되었다. 이들은 랜섬웨어의 다양한 변종을 만들었으며, 특히 OpenAI사의 ChatGPT를 활용해 랜섬웨어의 기능을 개선하고, 피해자의 네트워크에 취약점을 스캔해 공격을 수행했다고 밝혔다.

이처럼 AI기술이 급속으로 발전하며 GhatGPT를 통한 랜섬웨어 유지/보수 사례뿐만 아니라 피싱 공격 및 BEC[12] 공격에 사용되는 WormGPT[13] 및 FraudGPT[14], 구글 AI 챗봇 Bard의 다크웹 버전인 DarkBart, DarkBert를 통해 사이버 공격을 수행하는 시도가 지속적으로 확인되고 있다.

✓ **신규 랜섬웨어 및 그룹 활동**



[그림 3] 신규/변종 랜섬웨어 활동

2023년 11월, 8Base 그룹의 공격자가 서비스형 랜섬웨어인 Phobos 랜섬웨어를 사용해 공격을 수행하는 정황이 확인되었다. 또한 같은 달, CISA[15]에서는 ViceSociety 랜섬웨어를 사용하던 공격자가 Rhysida 랜섬웨어를 사용해 공격을 수행하고 있다는 내용과 함께 보안권고문을 발표했다. 이와 같이 오직 하나의 랜섬웨어 그룹과 제휴를 맺는 것이 아닌 여러 서비스형 랜섬웨어와 제휴를 맺고 공격을 수행하는 계열사 및 공격자들이 계속해서 늘어나는 추세이다.

Phobos 랜섬웨어는 2019년 1월에 발견된 이후 많은 변종이 파생되어 공격에 사용되고 있다. Phobos 랜섬웨어의 변종 중 vx-underground를 사칭한 랜섬웨어가 발견되었는데, vx-underground는 악성코드 저장소 웹사이트이자 X(트위터)를 통해 악성코드와 관련해 활발하게 활동하는 그룹이다. 해당 랜섬웨어가 발견되자 vx-underground는 "우리는

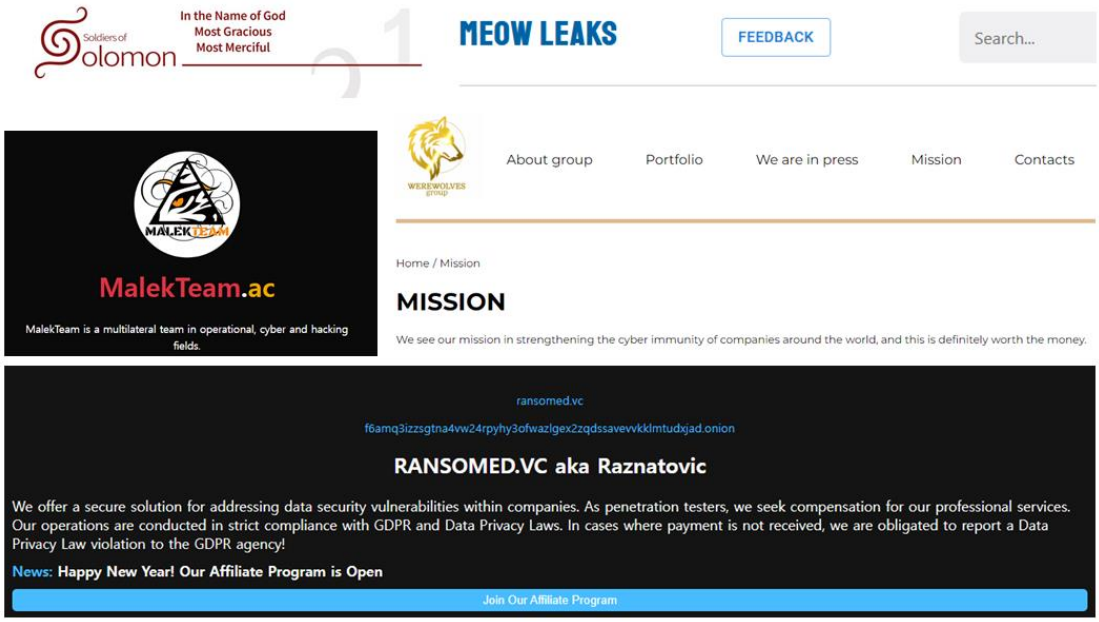
[12] BEC(Business Email Compromise): 사기꾼이 이메일을 통해 회사의 기밀 정보를 누설하도록 유도하는 사이버 범죄

[13] WormGPT: 피싱 및 BEC공격을 수행하기 위한 목적으로 개발된 AI 모델

[14] FraudGPT: 악성코드 작성, 피싱 페이지 생성 등의 악성행위를 수행하기 위한 목적으로 개발된 AI 모델

[15] CISA(Cybersecurity and Infrastructure Security Agency): 미국 국토안보부 산하기관으로, 미국의 사이버 보안 전담 기관

랜섬웨어를 사용하지 않으며 그런 오래된 랜섬웨어는 사용하지 않는다" 라고 얘기했다.



[그림 4] 신규 랜섬웨어 다크웹 활동

4분기에는 아래와 같이 총 7개의 랜섬웨어 그룹이 활동을 시작했다.

- **Soldiers of Solomon**

  2023년 10월부터 활동을 시작했으며, 친 팔레스타인 핵티비즘 그룹으로 주로 이스라엘의 시설 및 기관을 타깃으로 공격을 수행하고 있다. 이들은 탈취한 데이터를 다크웹 포럼을 통해 공개하고 있으며 추가로 텔레그램 메신저와 X(트위터)를 통해 공격의 기록을 남기고 있다. 한편 이들은 서비스형 랜섬웨어인 Crucio 랜섬웨어를 사용해 공격을 수행하고 있다.

- **Hunters International**

  2023년 10월부터 활동을 시작했으며, 현재는 폐쇄된 Hive 그룹의 랜섬웨어와 Hunters에서 사용하는 랜섬웨어 간에 약 56% 이상의 코드 유사성이 확인된 점 및 Hunters 랜섬노트에 기재된 다크웹 사이트의 백엔드 코드가 Hive 그룹에서 사용하던 다크웹 사이트와 상당히 유사하다는 추측이 나오면서 Hive 그룹의 리브랜딩[16]으로 추정되고 있다. 하지만 Hunters 그룹은 이러한 시선을 의식한 듯 그들의 다크웹을 통해 "세간의 추측은 틀렸으며, 단지 Hive 그룹이 판매한 소스코드를 구매했을 뿐" 이라는 내용의 글을 게시했다.

- **Meow**

  2022년 8월부터 활동을 시작한 그룹으로 2023년 2월부터 휴식기를 거쳐 11월부터 다시 활동을 하기 시작했다. 해당 그룹은 ChaCha20 및 RSA-4096 알고리즘을 사용하는 Conti v2 변종 랜섬웨어를 사용해 공격을 수행하

[16] 리브랜딩: 랜섬웨어 그룹이 운영을 중단한 뒤 새로운 이름으로 다시 복귀 또는 운영하는 행위

고 있으며, 3월에는 다크웹 포럼에 미상의 인물이 Meow 랜섬웨어 공격에 사용된 257개의 복호화 키, 복호화 도구, 복호화 도구 소스코드를 게시해 Kaspersky에서 해당 내용을 기반으로 복호화 도구를 배포한 이력도 있다.

- **WereWolves**

  2023년 12월부터 활동을 시작한 그룹으로, 러시아어를 사용하며 러시아 기업들을 타깃으로 공격을 수행하고 있다. "전 세계 기업의 사이버 면역성을 강화하는 것이 우리의 사명이라고 생각한다"는 이들은 LockBit 그룹과 유사하게 웹사이트, 랜섬웨어에 대한 버그바운티[17]를 진행하고 있으며 랜섬웨어 그룹 관계자에 대한 Doxing[18]에 성공할 경우 포상금도 제공하고 있다.

- **DragonForce**

  2023년 12월부터 활동을 시작한 그룹으로, 같은 달 야구르트 호주 지사의 데이터 유출을 통해 이슈가 되었다. 이들은 친 팔레스타인 핵티비스트 그룹인 DragonForce Malaysia와는 별개이며, 새롭게 나타난 랜섬웨어 조직임에도 불구하고 공격 전략, 협상 스타일, 데이터 유출 사이트 등을 기반으로 보았을 때 경험이 풍부한 것으로 판단된다.

- **Raznatovic**

  2023년 12월부터 활동을 시작한 그룹으로, 이들의 데이터 유출 사이트에 "RANSOMED.VC aka Raznatovic" 문구가 게시돼 있는 것이 특징이다. RansomedVC 그룹은 폐쇄하기 전인 10월 30일, 수사기관들의 감시로 두려움을 느끼고 있으며 모든 프로젝트를 팔고 싶다는 게시글을 올린 뒤 11월 8일에 6명의 관계자가 체포되고 98개의 계열사를 해고하며 운영을 중단했는데, Razatovic 그룹에서 해당 그룹의 인프라를 구매하여 사용하고 있는 것으로 추측된다.

- **MalekTeam**

  2023년 12월부터 활동을 시작한 그룹으로, 주로 이스라엘 기업 및 시설을 타깃으로 공격을 수행하고 있다. 다크웹 데이터 유출 사이트에는 이스라엘 군사 관련 기관, 병원 등을 공격 후 6건의 데이터를 게시하였으며, 이러한 점을 통해 이스라엘과 적대관계에 있는 이란의 공격 그룹으로 추측되고 있다.

[17] 버그바운티: 소프트웨어 또는 웹서비스의 취약점을 찾아낸 사람에게 포상금을 지급하는 제도

[18] Doxing: dropping docx(문서를 떨어뜨리다)에서 파생된 단어로, 특정인의 신상정보를 온라인에 공개하는 행위를 뜻함

BlackCat History

[그림 5] BlackCat 그룹의 폐쇄된 다크웹 사이트(일부)

BlackCat 그룹은 BlackCat, ALPHV, Noberus 등 3개의 이름으로 알려져 있다. 그 중 BlackCat이란 이름은 랜섬웨어를 판별할 수 있는 ID Ransomware를 운영하는 Malware HunterTeam과 사이버 보안 회사인 Recorded Future에서, Noberus는 미국의 보안 소프트웨어 회사 Symantec에서 명명한 이름이며, 실제 그들은 스스로를 ALPHV라고 말하고 있다. BlackCat 그룹은 2021년 11월부터 활동을 시작한 그룹으로 2022년에는 227건, 2023년에는 431건의 피해자를 만들어내며 LockBit 그룹 다음으로 가장 활발하게 공격을 수행해왔다.

이들은 러시아어에 능통한 계열사만을 모집했으며 랜섬웨어 공격 시에도 PC에서 사용하는 언어를 확인해 CIS(독립국가연합) 언어를 사용하고 있을 경우 공격을 수행하지 않아 러시아에 본거지를 둔 그룹으로 추정되고 있다. 또한 BlackCat 랜섬웨어는 당시 발견된 랜섬웨어 중 최초의 Rust 언어 기반 랜섬웨어로 큰 이슈가 되었다.

BlackCat 그룹은 활동을 시작한지 얼마되지 않아 많은 피해자들을 만들어 내고 가장 활발한 랜섬웨어 그룹의 반열에 올랐는데, 이는 타 그룹에 비해 계열사에게 높은 수익률을 보장함으로써 짧은 시간에 많은 계열사를 모집했기 때문으로 볼 수 있다. 현재 가장 활발하게 공격을 수행하고 있는 LockBit 그룹 계열사의 수익률이 공격을 통해 얻은 몸값의 70%인 것을 감안했을 때 BlackCat 그룹 계열사의 수익률이 몸값의 최대 90%인 것은 상당히 파격적인 조건으로 볼 수 있다.

BlackCat 그룹의 랜섬웨어는 Windows, Linux를 타깃으로 공격이 가능한 Version1, Version2, Version3, BlackCat Sphynx를 출시했으며, 난독화를 적용하여 백신을 우회하기위해 제작한 ALPHV MORPH 변종, 안전모드에서 재부팅을 실행하는 SafeBoot 변종 등 다수의 BlackCat 랜섬웨어 변종이 발견되기도 했다.

이들이 사용했던 협박 전략 또한 눈여겨볼 만하다. 데이터를 암호화하고 파일 유출을 빌미로 이중 협박 전략을 사용하

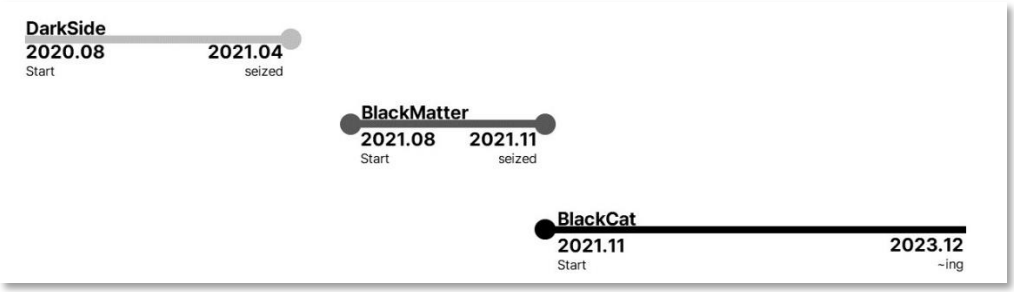
고, 피해 기업에 대한 상세정보를 얻어올 수 있는 크롤러와 API를 지원하기 시작했고, 타이포스쿼팅[19]을 통한 피해기업 데이터 유출, 몸값을 지불하지 않은 피해기업들을 SEC(미국 증권거래위원회)에 고소하는 등의 행태를 보이기도 했다.

한편 BlackCat 그룹은 DarkSide/BlackMatter 그룹의 리브랜딩으로 알려져있다. BlackCat 그룹의 활동을 시작하자 LockBit 그룹에서 가장 먼저 의구심을 제기했고, 이 외에도 BlackMatter 그룹에서만 사용되던 데이터 유출 도구 ExMatter가 BlackCat 랜섬웨어 공격에 사용된 점, BlackMatter 랜섬웨어 공격에서 사용된 C2 서버[20] IP가 BlackCat 랜섬웨어 공격에서도 확인된 점, 그리고 결론적으로 FBI의 Flash 보고서[21]에서 BlackCat 그룹의 여러 개발자와 자금 세탁자가 DarkSide/BlackMatter 그룹과 연결되어 있다고 공식적으로 보고되었다.

2023년 12월, BlackCat 그룹의 데이터 유출 사이트에 FBI의 압수 포스터가 게시되며 그룹의 활동이 종료되는 듯싶었으나, 인프라를 다시 복구 후 활동을 이어가고 있는 상황이다. 더군다나 이들은 FBI에 대한 보복을 목적으로 기존에는 금지되어 있던 핵심 인프라에 대한 공격을 허용했기 때문에, 위협이 더욱 커질 수 있을 것으로 보인다.

1. BlackCat과 DarkSide/BlackMatter와의 연관성

- **BlackMatter, DarkSide, BlackCat 그룹의 활동 시기**



[그림 6] DarkSide, BlackMatter, BlackCat 활동 시기

DarkSide 그룹은 2020년 8월부터 활동을 시작한 그룹으로, 2021년 4월까지 활동하다 미국 법무부 및 FBI의 압력으로 데이터 유출 사이트가 폐쇄되고 피해자들로부터 갈취한 몸값이 압수되며 활동을 중단했다. 이후 DarkSide 그룹이 폐쇄된 지 4개월 뒤인 2021년 8월에 BlackMatter 그룹 또한 4개월간의 활동을 수행한 뒤 수사기관의 압력으로 인해 운영을 중단하겠다고 선언하고 그룹을 폐쇄했다. BlackMatter 그룹이 폐쇄된 직후에는 곧이어 BlackCat 그룹이 11월 말부터 활동을 시작했다. 이와 같이 그룹들의 활동 시작 및 폐쇄 타이밍이 모두 적절하게 이어져 있어 세 그룹의 연관성을 볼 수 있다.

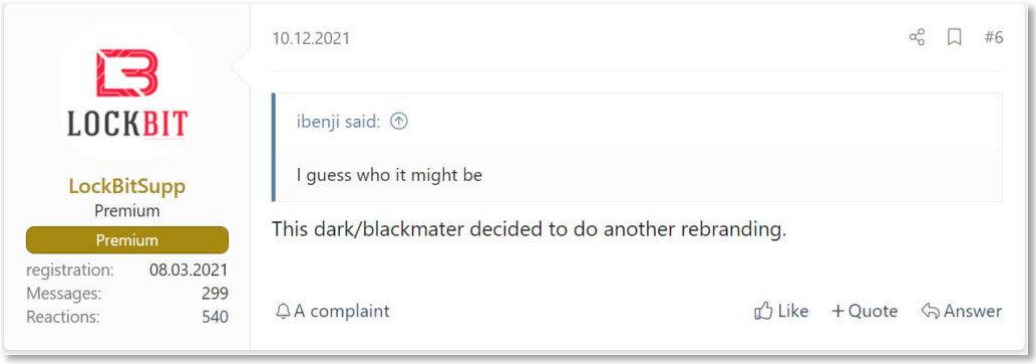
한편 BlackCat 그룹의 활동이 시작되자, LockBit 그룹은 "BlackCat 그룹은 DarkSide/BlackMatter 그룹의 리브랜딩이다" 라는 글을 포럼에 게시해 이슈가 되기도 했다.

---

[19] 타이포스쿼팅(TypoSquatting): 철자가 틀린 도메인 이름을 사용해 가짜 도메인을 합법적인 도메인으로 속이는 행위

[20] C2 서버: 공격자가 초기 침투에 성공한 기기와의 통신을 유지하는데 사용하는 서버

[21] FLASH(FBI Liaison Alert System) 보고서: 사이버 위협에 대응하기 위해 FBI에서 발간하는 보고서



[그림 7] BlackCat 그룹에 대한 LockBit의 의견

- **BlackMatter 랜섬웨어 공격에 ExMatter 탈취 도구 사용**

ExMatter는 BlackCat 그룹에서 데이터를 탈취하기 위해 사용하는 것으로 알려진 해킹 도구이다. ExMatter는 Ryuk 그룹이 사용한 Ryuk Stealer, LockBit 그룹이 사용하는 StealBit 이후로 발견된 Custom 데이터 탈취 도구로 확인되었는데, 2021년 11월 BlackMatter 그룹의 공격에서도 ExMatter 정보 탈취 도구가 사용된 정황이 확인되었다. 기존에 알려지지 않은 도구였음에도 불구하고 두 랜섬웨어 공격에 사용했다는 점에서 연결점이 일부 확인된다.

- **BlackCat 그룹, DarkSide/BlackMatter 그룹의 계열사로 시작**

BlackCat 그룹은 Recorded Future와의 인터뷰에서 "우리는 단지 DarkSide/BlackMatter 그룹의 계열사에서 시작한 그룹이다"라고 밝혔다. 하지만 보안 연구원들은 수사기관에 압력으로 인해 폐쇄된 DarkSide, BlackMatter 그룹의 평판으로 인해 이를 부정하는 것으로 볼 수 있다는 의견을 내고 있다.

- **BlackMatter 랜섬웨어 공격에 사용된 C2, BlackCat 랜섬웨어 공격에서도 발견**

2021년 12월 발생한 BlackCat 랜섬웨어 공격에서 사용된 C2가 2021년 9월 BlackMatter 공격에서도 사용된 것이 확인되었다. 특히 2021년 12월은 BlackCat 그룹이 활동을 시작한지 얼마되지 않은 때였는데, BlackMatter가 BlackCat으로 리브랜딩 하자마자 BlackMatter의 계열사들이 BlackCat 그룹과 제휴를 맺었을 가능성이 있지만, 랜섬웨어 계열사들이 여러 랜섬웨어의 계열사로 활동하는 사례도 있어 해당 사례만으로는 정확한 증거로 보기는 어렵다.

- **FBI Flash Report**

2022년 4월에 발간된 FBI Flash 보고서에는 BlackCat 랜섬웨어 그룹의 여러 개발자와 자금세탁자가 DarkSide/BlackMatter 그룹과 연결되어 있다고 언급했으며, 이를 통해 BlackCat 그룹이 랜섬웨어 운영에 대한 광범위한 네트워크와 경험을 보유하고 있음을 알 수 있다.

2. BlackCat 그룹 이슈

- **BlackCat, 첫 발견**

[그림 8] BlackCat 랜섬웨어 첫 발견

2021년 11월, MalwareHunterTeam에 의해 처음으로 BlackCat 랜섬웨어 샘플이 발견되면서 해당 그룹의 존재가 알려졌으며, 현재까지 확인된 랜섬웨어 중 처음으로 발견된 Rust 언어 기반의 랜섬웨어였기 때문에 큰 이슈가 되었다.

- **러시아 다크웹 포럼을 통해 계열사 및 침투 테스터 모집**

2021년 12월, BlackCat 그룹은 해킹 포럼인 XSS 및 Exploit 포럼에서 alphv라는 닉네임으로 계열사를 모집하고, 러시아 사이버 범죄 포럼인 RAMP에서 ransom이라는 닉네임으로 활동하며 침투 테스터를 모집하는 등 활동 영역을 넓혀가는 모습을 보였다.

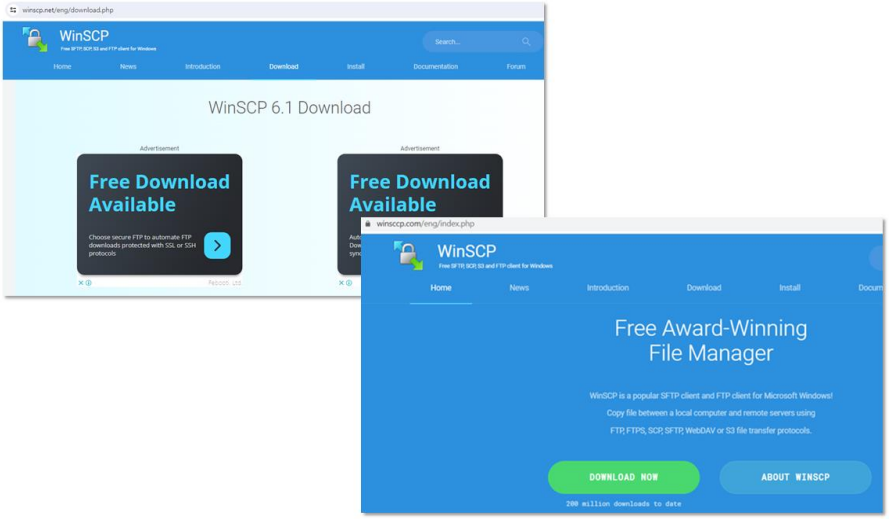
- **BlackCat 계열사, Veritas Backup Exec 취약점 사용**

보안업체 Mandiant에 의하면 Veritas Backup Exec의 공개된 취약점(CVE-2021-27876, CVE-2021-27877, CVE-2021-27878)을 악용하여 BlackCat 랜섬웨어 공격이 2022년 10월부터 발견되었다고 밝혔다. 해당 취약점은 2021년 3월에 패치된 취약점이며, 2022년 9월 23일 침투 테스트 프레임워크인 Metasploit에 추가되었다. 해당 공격을 수행한 BlackCat 그룹의 계열사는 UNC4466으로 알려져 있으며, 이들은 Metasploit을 활용해 Veritas Backup Exec 솔루션을 사용하고 있는 Windows 서버에 침투해 랜섬웨어 공격을 수행한 것으로 확인됐다.

- **Malvertising을 통한 BlackCat 랜섬웨어 공격 수행**

Malvertsing은 Malicious(악성)와 Advertising(광고)의 합성어로, 온라인 광고를 통해 악성코드를 유포시키는 행위를 뜻한다. 이러한 유형의 악성코드 유포 사례가 BlackCat 그룹에서도 사용된 사례가 발견되었다. 2023년 7월 이들은 Google에서 제공하는 광고서비스인 Google Ads를 통해 Advanced IP Scanner, Slack, WinSCP, Cisco AnyConnect 등의 인기 소프트웨어로 위장해 광고를 한 뒤, 실제로 해당 파일을 다운로드 받고 실행할 경

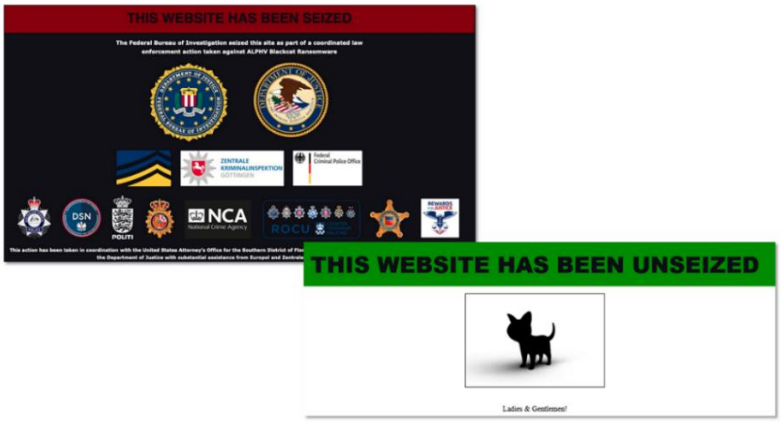
우에는 Nitrogen 악성코드가 실행되도록 설계가 되어 있었다. Nitrogen악성코드는 CobaltStrike Beacon[22]을 다운로드 한 뒤 추가 악성코드들을 실행시키는 악성코드이며, 이후 설치되는 악성코드들을 통해 최종적으로 BlackCat 랜섬웨어를 배포해 공격을 수행한 것으로 확인된다.



[그림 9] winscp.net, winsccp.com

Malvertising을 통해 BlackCat 랜섬웨어를 유포한 사례와 비슷하게, 2023년 6월에는 Windows용 WinSCP 파일 전송 애플리케이션의 공식 웹사이트(winscp.net)를 모방한 가짜 페이지(winsccp.com)로 사람들을 유인한 뒤 파일 다운로드 시 정상 파일로 위장한 CobaltStrike Beacon을 다운로드 후 BlackCat 랜섬웨어 공격을 수행한 사례도 발견되었다.

- **데이터 유출 사이트 Seized, Restore**

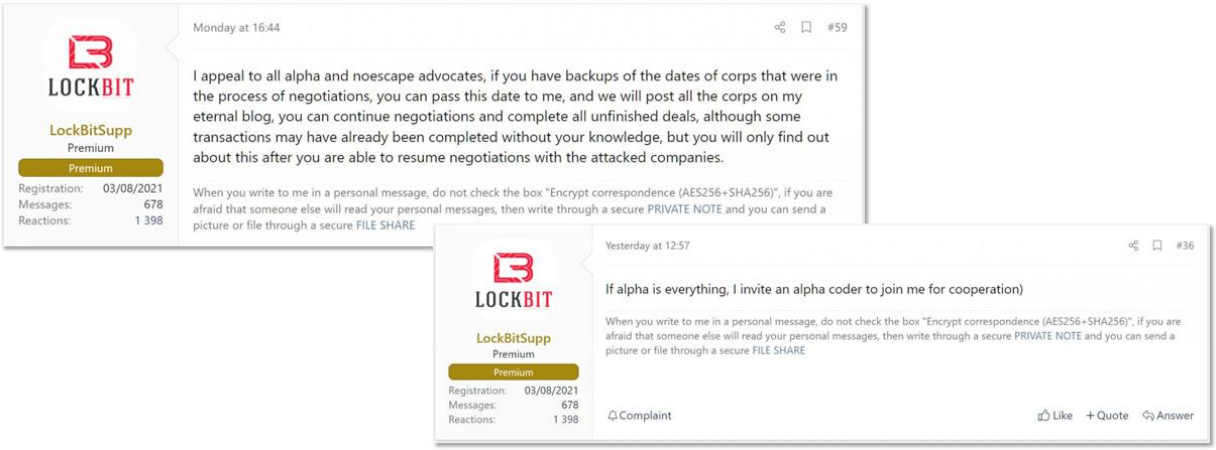


[그림 10] FBI vs BlackCat

[22] CobaltStrike Beacon: 모의해킹 도구인 CobaltStrike에서 사용되는 정보 수집, 명령 실행 등의 작업을 수행할 수 있는 파일 또는 백도어

2023년 12월 7일, BlackCat 그룹의 데이터 유출 사이트가 접속이 불가능해졌다. 이후 BlackCat 그룹의 관리자는 사이트의 운영이 다시 재개될 것이라고 했으나 12월 19일, BlackCat 그룹의 데이터 유출 사이트에 FBI 압수 포스터가 게재된 후 곧이어 FBI의 공식성명이 발표되며 BlackCat 그룹의 폐쇄가 확정되는 듯했다. 하지만 같은 날 BlackCat 그룹은 데이터 유출 사이트를 복구한 뒤 FBI가 하나의 데이터 센터에 접근하였으며 획득한 키는 한 달 반 동안 사용된 키로 약 400여개 회사에 해당되며, 3,000개가 넘는 회사는 더 이상 키를 받을 수 없고 FBI의 행동으로 미국 및 관련 기관에 대한 공격을 계열사들에게 허용하겠다는 글을 게시했다. 이후 데이터 유출 사이트는 계속해서 폐쇄, 복구되며 FBI와 BlackCat 그룹의 신경전이 이어졌으나, BlackCat 그룹은 데이터 유출 사이트를 다시 개설한 뒤 새로운 피해자들을 게시하고 있다.

- **LockBit 그룹, BlackCat 그룹의 계열사 및 개발자 포섭 시도.**



[그림 11] LockBit 그룹의 BlackCat 계열사, 개발자 포섭

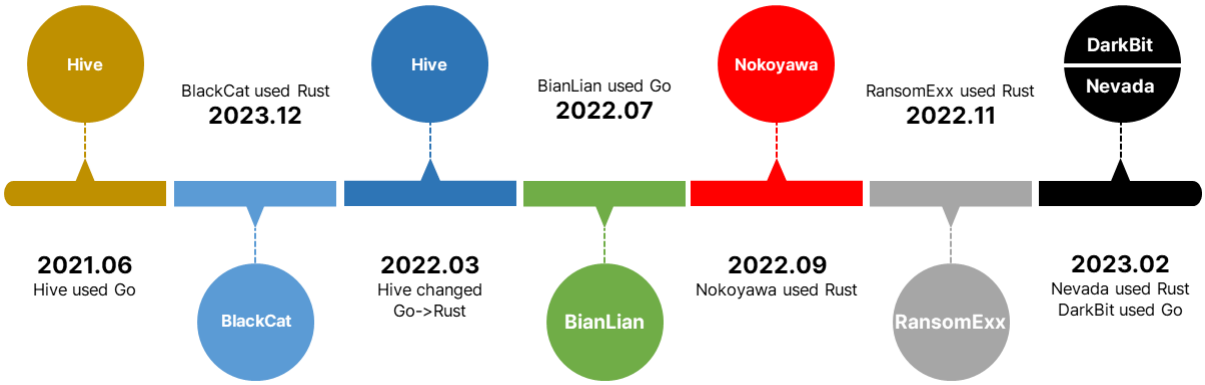
BlackCat 그룹의 폐쇄의 조짐이 보이자, LockBit 그룹은 BlackCat 그룹의 계열사와 개발자를 포섭하기 시작했다. 특히 LockBit 그룹은 다크웹 포럼에서 "BlackCat 그룹에서 LockBit 그룹으로 넘어온 파트너들을 존경한다", "그들은 익숙한 소프트웨어로 일하는 것을 원하고 있다"라는 글을 게시하며 개발자를 포섭하는 글을 게시했는데, 실제로 BlackCat 그룹 데이터 유출 사이트에 게시되었던 독일 에너지청이 LockBit의 데이터 유출 사이트에 등록되기도 했다. 이를 통해 BlackCat 그룹의 일부 계열사들이 이미 LockBit 그룹으로 넘어간 것으로 추측할 수 있다.

3. BlackCat 랜섬웨어 및 ExMatter 업데이트

- **처음으로 발견된 Rust기반 랜섬웨어**

  BlackCat 랜섬웨어는 2021년 11월 발견된 랜섬웨어이며, 현재까지 확인된 랜섬웨어 중 가장 처음으로 발견된 Rust 언어 기반의 랜섬웨어이다. BlackCat 그룹은 Recorded Future와의 인터뷰에서 왜 Rust 언어를 사용해 랜섬웨어를 제작했냐는 질문에 "우리는 단지 현대적인 요구사항을 충족하는 새로운 접근 방식으로 새로운 랜섬웨어를 만들었다"라고 진술했다. 하지만 단순히 현대적인 요구사항을 만족하기에는 Rust 언어 기반

의 BlackCat 랜섬웨어는 악성코드로서 많은 장점을 가지고 있다.



[그림 12] 랜섬웨어 그룹 비주류 언어 사용 현황

Rust 언어는 2015년 Mozilla에서 공식적으로 배포한 언어로, C/C++로 제작된 실행 파일과 같이 빠른 실행 속도를 가지고 있을 뿐만 아니라 메모리 충돌로 인한 오작동을 방지할 수 있는 장점이 존재한다. 따라서 이러한 장점을 악용해 랜섬웨어를 개발하게 되면 오류 없이 빠른 속도로 파일을 암호화할 수 있게 되며, 컴파일러에 의해 추가되는 메모리 로직으로 인해 분석을 지연시키고 탐지 회피의 가능성을 높일 수 있게 된다. 더 나아가 Rust 언어는 크로스 컴파일 언어로, 운영체제에 종속 받지 않고 다양한 운영체제를 타깃으로 실행파일을 생성할 수 있기에 최근 일부 랜섬웨어 그룹에서 사용되고 있는 추세이다.

- **정보 탈취 도구 ExMatter**

ExMatter는 BlackCat 그룹에서 사용한 정보 탈취 도구로, 랜섬웨어 공격 이전에 사용되며 지정된 디렉터리에서 지정된 확장자의 파일들을 찾아 사전에 구성된 서버에 SFTP를 통해 업로드 하도록 설계되어 있는 것이 특징이다.

이후 2022년 8월, BlackCat 그룹은 기능이 업데이트된 ExMatter를 사용해 공격을 수행하는 정황이 확인되었다. 업데이트된 ExMatter는 기존의 기능에서 FTP 프토토콜 지원, 탈취한 파일의 목록을 보여주는 보고서 작성 기능, 파일들을 손상시키는 기능, 자가 삭제 기능 등이 추가되었다.

한편 ExMatter는 2021년 11월 BlackMatter 그룹의 공격에서 사용되면서 발견되었던 도구로 Ryuk 그룹이 사용하는 Ryuk Stealer, LockBit 그룹이 사용하는 StealBit 이후로 발견된 Custom 데이터 유출 도구이며 2021년 11월 BlackMatter 그룹의 공격에서도 사용된 것으로 확인된다.

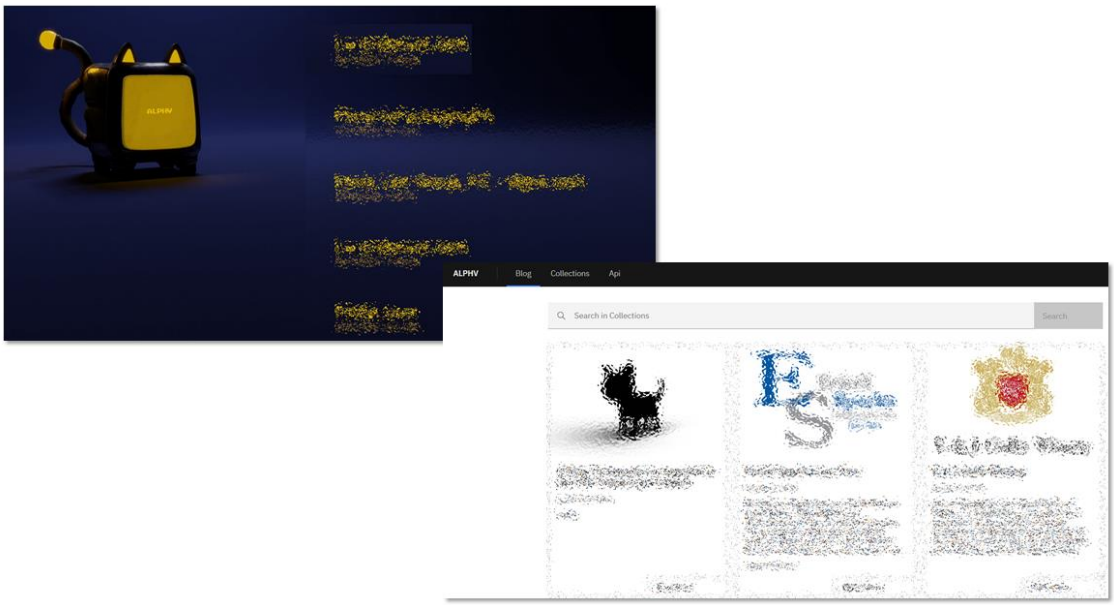
- **2023년 2월, BlackCat 2.0 Sphynx 버전 업데이트**

2023년 2월, BlackCat 2.0 Sphynx가 업데이트되었다. 기존 Version1에서는 랜섬웨어를 실행시키기 위해 access token 인자가 필요했으나 이를 삭제했고, 랜섬웨어 실행 시 암호화할 확장자, 종료할 프로세스, 암호화 방식 등 여러가지 설정 값을 가지고 있는 Config 값을 기존 버전의 Json 형태가 아닌 일반 문자열 형태로 변경했다. 또한 네트워크 사이에서 측면 이동을 수행할 수 있는 오픈소스 프레임워크 Impacket, 다른 장치에서 원격으로 명령을 실행할 수 있도록 하는 원격 쉘인 Remcom이 내장되었다.

BlackCat 그룹은 해당 랜섬웨어 업데이트에 "소스코드를 완전히 재 작성했다", "이번 업데이트는 AV[23] 및 EDR[24] 탐지를 최소화하는데 우선순위를 두었다" 라고 밝혔다.

4. 데이터 유출 및 협박 전략 진화

- **데이터 유출 사이트 개설**



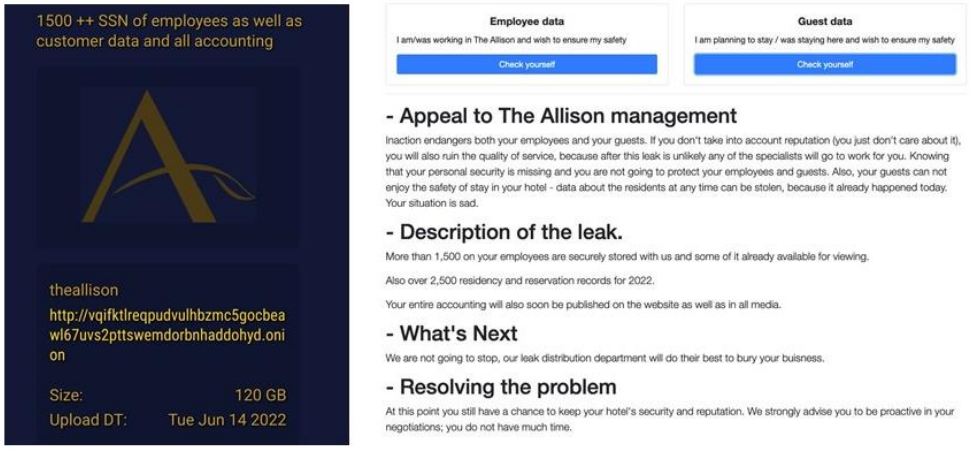
[그림 13] BlackCat 그룹 데이터 유출사이트 (과거/현재)

2021년 12월, BlackCat 그룹은 다크웹을 통해 계열사와 공격자를 모집하는 동시에 이중 협박을 수행하기 위한 데이터 유출 사이트를 개설했다. 이와 더불어 BlackCat 그룹은 DDoS 전략을 채택하여 3중 협박 전략을 사용하고 있다.

[23] AV(Anti-Virus): 바이러스 및 악성코드를 탐지하고 방어하기 위한 소프트웨어

[24] EDR(Endpoint Detection and Response): 컴퓨터 및 모바일과 같은 단말에서 발생하는 악성행위를 실시간으로 감지하고 대응하는 솔루션

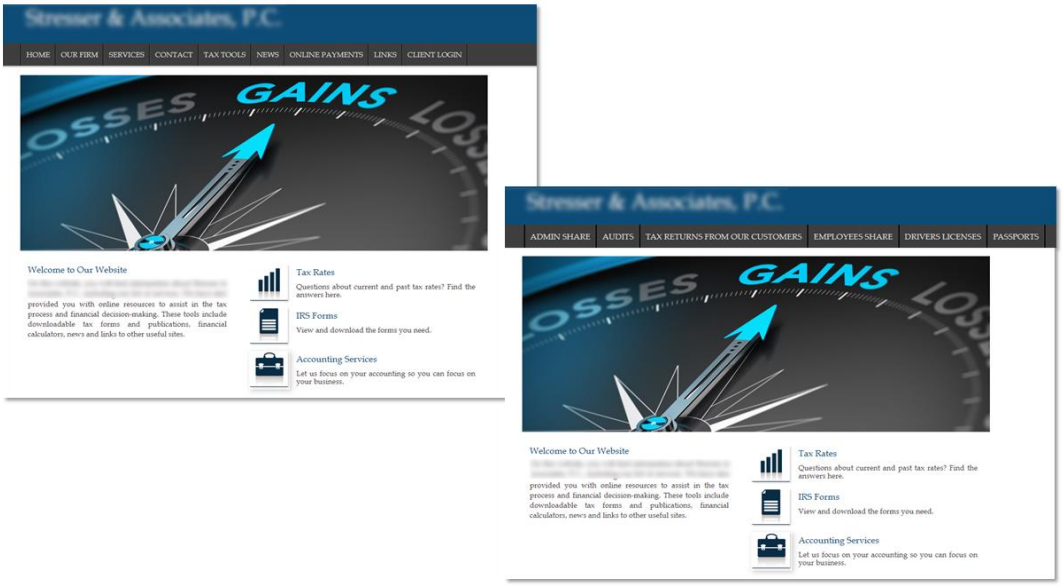
- **유출된 데이터를 검색할 수 있는 사이트 개설**



[그림 14] 다크웹 유출 및 검색 사이트 개설

2022년 6월, BlackCat 그룹은 Allison 호텔에서 탈취한 112GB의 데이터를 유출하기 시작했다. 이들은 해당 데이터를 유출 사이트에 게재 후 해당 호텔에서 유출된 직원 및 투숙객 1,500여명의 민감 정보를 검색할 수 있는 ClearNet[25]을 개설했다. 뿐만 아니라 검색엔진에서 상위에 노출될 수 있도록 해당 호텔과 관련된 데이터를 게시하였다. 이러한 사이트를 개설한 목적은 직원과 고객들에게 겁을 주어 해당 업체가 ClearNet에서 데이터가 삭제될 수 있도록 요구하려는 전략으로 볼 수 있다.

- **타이포스쿼팅을 통해 유인한 페이지에서 피해 기업의 데이터를 유출**

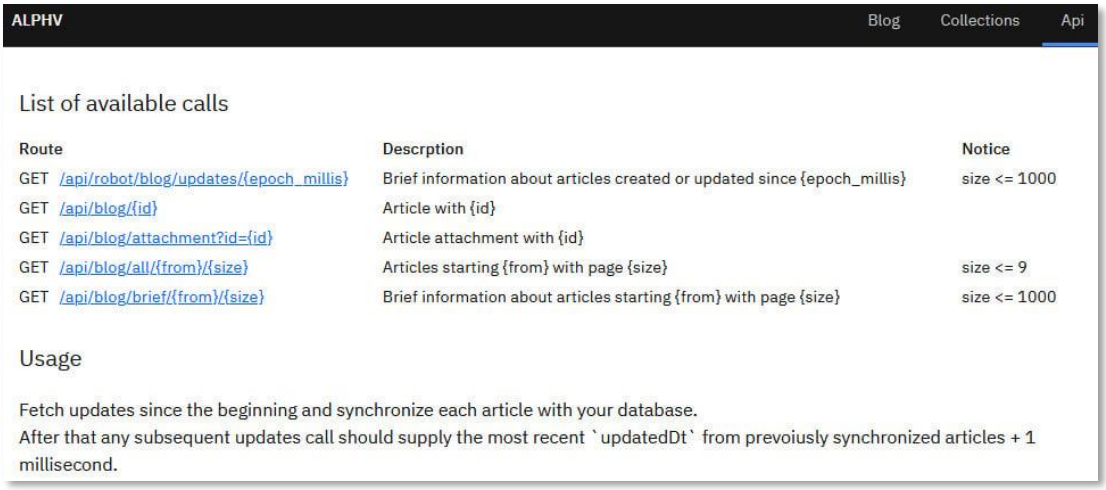


[그림 15] 타이포스쿼팅 및 피해 기업 웹 페이지 모방 (피해기업 페이지/BlackCat 데이터 유출 페이지)

[25] ClearNet: 누구나 공개적으로 접근할 수 있는 인터넷 또는 웹 사이트

2022년 12월, BlackCat 그룹은 금융회사를 데이터 유출 사이트 목록에 게시했으며, 몸값 협상이 이루어지지 않자 데이터를 유출하기 시작했다. 더 나아가 BlackCat 그룹은 해당 기업의 도메인과 유사한 도메인을 생성해 타이포스쿼팅을 유도했고, 피해 기업의 웹사이트까지 모방하여 직원 정보, 자산 및 지출 내역, 여권 등 3.5GB 크기의 데이터를 유출했다.

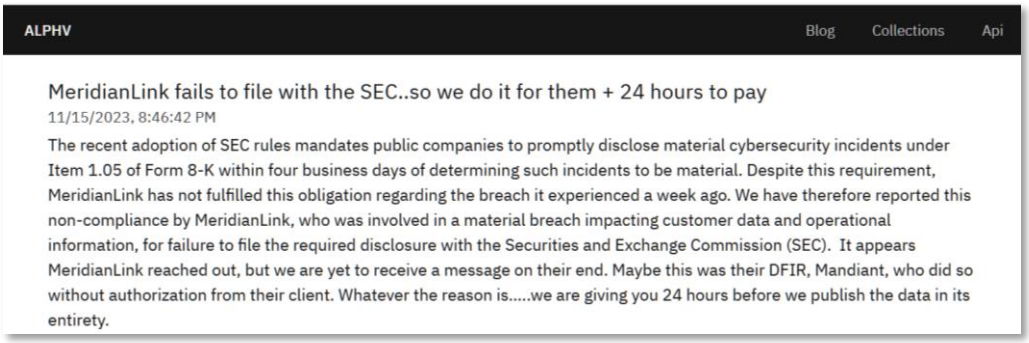
- **피해 기업의 상세정보를 얻어올 수 있는 API 제공**



[그림 16] 피해 기업의 상세정보를 얻어오는 API 제공

2023년 7월, BlackCat 그룹은 데이터 유출 사이트에 게시된 피해 기업에 대한 상세 정보를 가져올 수 있는 API를 지원하기 시작했으며, 해당 API를 사용할 수 있는 Python으로 작성된 크롤러를 제공하기도 했다. 이는 BlackCat 그룹에 몸값을 지불하는 피해자들이 감소하자 협박 수위를 올려 몸값을 받아내기 위한 목적으로 볼 수 있다.

- **몸값을 지불하지 않는 기업은 SEC(미국 증권거래위원회)에 고소**



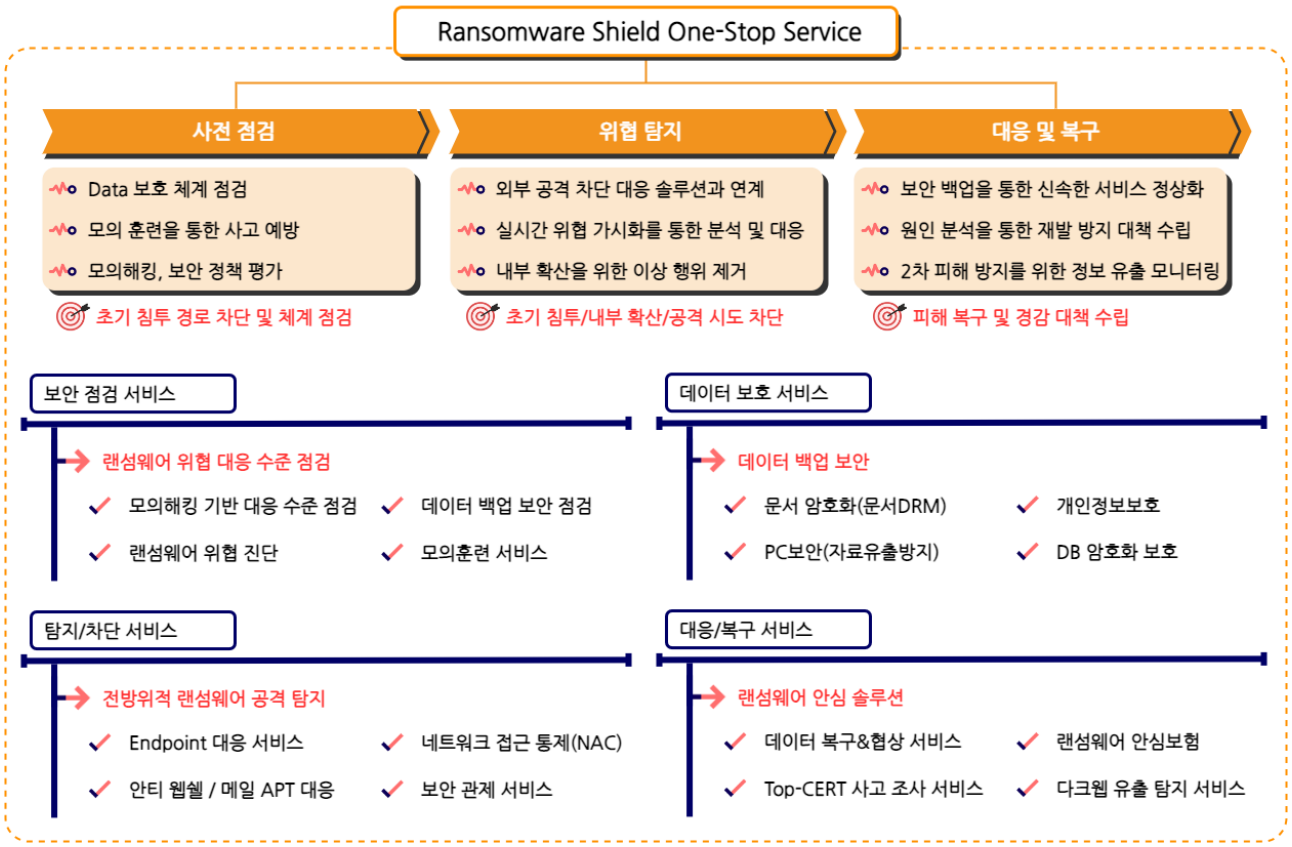
[그림 17] 피해기업 SEC에 고소 협박

2023년 11월, BlackCat 그룹은 소프트웨어 회사 MeridianLink를 데이터 유출 사이트에 게시하며, 24시간 내에 몸값을 지불하지 않으면 데이터를 유출하겠다고 협박을 하기 시작했다. 더 나아가 BlackCat 그룹은 MerdianLink 회사가 고객 데이터 및 운영 정보가 탈취당하는 사고가 발생했음에도 불구하고 SEC(미국 증권거래위원회)에 보고하지 않은 것에 대해 고소하겠다며 해당 고소장을 작성한 양식을 사진으로 게시했으며, 24시간 이후에도 몸값이 지불되지 않자 고소장을 제출한 사진을 게시했다.

이는 미국에서 사이버 사고가 연이어 발생하자 SEC(미국 증권거래위원회)에서 상장 기업이 중대한 영향 및 투자 결정에 영향을 미치는 사고가 발생할 시 4일 이내로 보고를 해야 한다는 점을 악용함으로써 몸값 지불을 유도하려는 전략으로 볼 수 있으나, 해당 규정은 2023년 12월 15일부로 발효될 예정이었으므로 실질적인 법적 효력은 없었던 것으로 알려졌다.

랜섬웨어 Mitigation

공격자는 공격대상을 선정하기위해 공격자 그룹이 수립한 전략을 통해 다양한 방법으로 정찰을 수행하며 이후 내부 인프라에 침입하여 파일을 암호화시키고 자산을 위협하며 데이터 유출을 통한 협박을 시도한다. 이러한 피해를 예방하기 위해 타깃형 APT 공격에 대한 대비와 침입에 대한 각 단계별 적절한 보안 요소 및 프로세스를 마련하여 공격자 그룹이 목표를 달성하기 전에 탐지하고 차단할 필요가 있다.

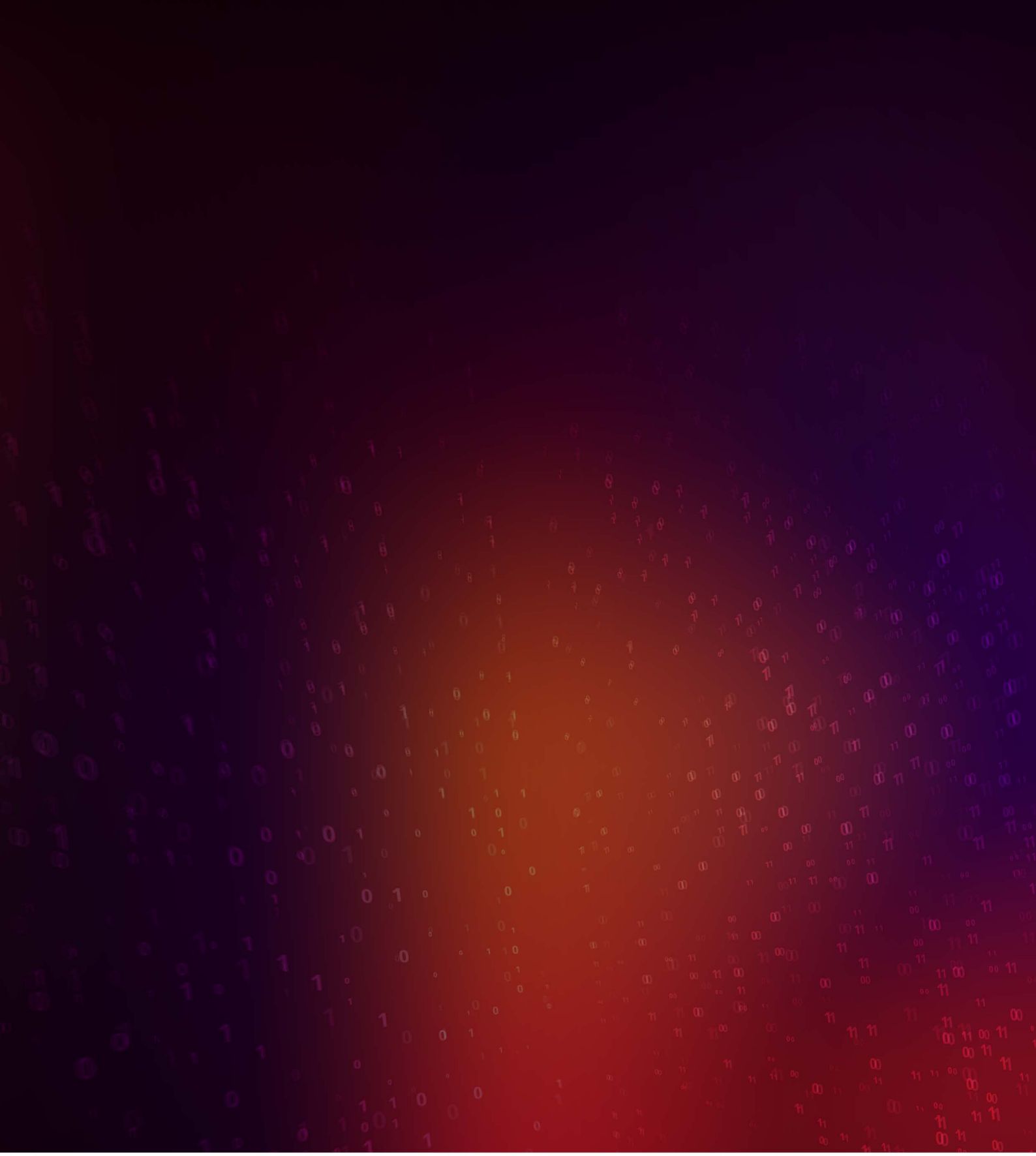


부록

랜섬웨어 그룹	활동 기간	설명
BlackCat	2021.12~	DarkSide/BlackMatter 리브랜딩 버전으로 현재까지 3번째로 많은 피해자가 발생한 대형 그룹
BlackMatter	2021.07~2021.11	Exploit 포럼을 통해 공개되었으며, DarkSide의 리브랜딩 버전으로 FBI 등 수사 기관의 압박으로 활동 종료
BlackSuit	2023.05~	23년 12월 국내 골프관련 소프트웨어 개발 업체 데이터를 다크웹에 공개한 이력이 있는 그룹
Cactus	2023.03~	랜섬웨어 동작에 필요한 데이터가 암호화되어 있어 실행 시 복호화 키가 필요하여 탐지 회피 전략 구사
Cerber	2016.03~2017.09	다양한 버전(1~6.0.1)이 존재하며, 주로 광고 서비스의 정상적인 네트워크를 이용하여 유포하여 불특정 다수를 대상으로 공격을 수행
Clop	2019.02~	복호화 툴 공개 이후 데이터 탈취에 집중하여 취약점을 통한 대규모 공격을 주요 전략으로 삼으며, 현재까지 4번째로 많은 피해자가 발생한 대형 그룹
DarkSide	2020.08~2021.05	21년 5월 미국 최대 송유관 중 하나인 콜로니얼 파이프라인을 공격하여 대규모 피해를 입혔으며, 이 후 FBI에 의해 암호 화폐 회수 및 활동 종료
Dharma	2016.11~	CrySis 랜섬웨어의 변종으로 암호화 후 변경되는 확장자가 변경되어 지속 발견 중인 가운데 23년 12월 Dharma 랜섬웨어를 사용하는 그룹 총책 체포
DragonForce	2023.12~	야쿠르트 호주 지사 공격 후 95GB 상당의 데이터 유출 및 오하이오 복권 시스템 공격 후 약 600GB 탈취한 이력이 있는 그룹
GhostSec	2015~	이슬람 극단주의 단체를 공격하기위해 형성된 그룹으로 23년 10월 텔레그램 메신저를 통해 GhostLocker 서비스형 랜섬웨어 판매하기 시작한 그룹
HelloKitty	2020.11~	침투 테스트 도구인 CobaltStrike 혹은 피싱과 아파치 서버의 취약점을 악용하여 공격을 수행한다. 23년 10월 2020년 버전의 소스 코드 유출
Hive	2021.06~2023.01	다양한 버전(1~6)이 존재하며 일부 버전은 복호화가 가능하다. 가장 활동적인 대형 그룹 중 하나였지만 '23년 1월 FBI에 의해 폐쇄
Hunters	2023.10~	Hive 랜섬웨어와 일부 연관성이 제기되는 그룹으로 Hive 랜섬웨어 v6 버전과 약 56% 코드 유사성 확인
LockBit	2019.10~	현재까지 가장 영향력 있는 랜섬웨어 그룹으로 여러 버전 업데이트를 거쳐 LockBit 3.0을 운영하고 있으며, 이력서/저작권 관련 피싱을 통해 국내 공격 지속
LockerGoga	2019.01~2021.10	추정 피해액 약 1억 400만 달러를 발생시킨 그룹으로21년 10월 LockerGoga, MegaCortex를 같이 운영하던 공격자가 체포되었고, 22년 9월 복호화 툴 제공

MalekTeam	2023.12~	이란 해커 그룹으로 이스라엘, 시온주의를 비방하며 이스라엘 군사 관련 기관, 병원 등을 공격
MegaCortex	2019.01~	21년 10월 LockerGoga, MegaCortex를 같이 운영하던 공격자가 체포되었으며, 23년 1월 복호화 툴 제공
Meow	2022.08~	2020년 9월에 유출된 Conti 랜섬웨어의 소스코드를 사용해 공격을 수행하는 그룹
NoEscape	2023.06~2023.12	암호화 방식 및 랜섬웨어의 유사성으로 인해 21년에 운영을 중단한 Avaddon 그룹과의 연관성이 확인되는 그룹으로 23년 12월에 그룹 운영자가 Exit Scam 후 도주하며 운영 중단
Phobos	2018.12~	Dharma 랜섬웨어의 변종이며 주로 취약한 패스워드를 사용중인 RDP 포트로 초기 침투해 공격 수행
Qilin	2022.10~	23년 11월 국내 전자부품 제조업체 데이터를 다크웹 유출 사이트에 공개한 이력이 있는 그룹
RagnarLocker	2019.12 ~ 2023.10	취약한 RDP포트로 초기 침투해 공격을 수행하는 그룹으로 23년 10월에 Europol에 의해 핵심인력이 체포되며 활동 중단
RansomedVC	2023.08~2023.11	Stormous, Everest 그룹과 협력관계를 맺었으며 23년 11월 초 수사기관의 압박으로 인해 관계자가 체포되고 운영 중단
Raznatovic	2023.12~	23년 11월 폐쇄된 그룹인 RANSOMEDVC 그룹의 인프라를 구매하여 사용하고 있는 그룹
Rhysida	2023.05~	23년 5월 칠레군의 기밀 문서를 데이터 유출 사이트에 게시한 이력이 있는 그룹
SiegedSec	2022.04~	GhostSec 그룹과 협력관계에 있는 그룹으로 SQL 인젝션 및 XSS취약점을 악용해 공격을 수행하고 다크웹 포럼을 통해 데이터를 유출하는 그룹.
Soldiers of Solomon	2023.10~	친 팔레스타인 핵티비즘 그룹으로 서비스형 랜섬웨어인 Crucio 랜섬웨어를 사용하며 이스라엘의 시설 및 기관을 타깃으로 공격을 수행하는 그룹
Trigona	2023.04~2023.10	친 러시아 성향을 띄고 있는 랜섬웨어 그룹으로 23년 10월 17일 우크라이나 사이버 동맹(UCA)에 의해 운영 중단
ViceSociety	2021.05~	러시아어를 사용하고 있으며 활동 초기에는 교육 산업군을 집중적으로 공격 했으나 현재는 다양한 산업군을 타깃으로 공격을 수행중인 그룹
WereWolves	2023.12~	러시아 기업들을 타깃으로 공격을 수행하는 그룹으로, 가장 영향력 있는 LockBit 그룹과 유사하게 웹사이트 및 랜섬웨어 버그바운티를 진행하고 있는 그룹

[표 2] 랜섬웨어 및 그룹 설명



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